Anonymity and censorship circumvention with Tor

Lunar <lunar@torproject.org>

July 8th, 2013 — LSM2013, Brussels

What is this Tor thing?

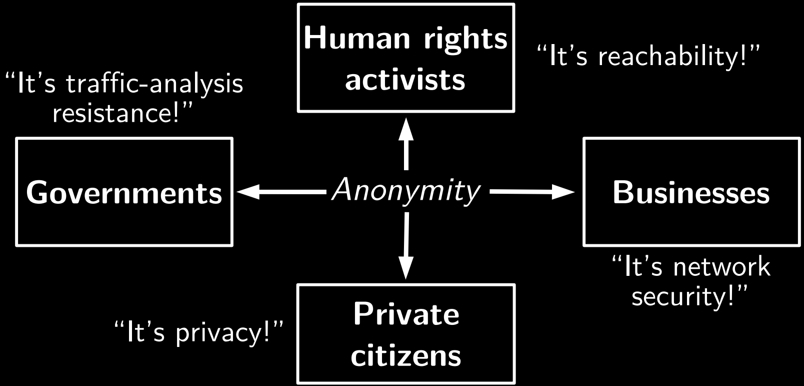
Tor helps people

Estimated 500,000 daily Tor users

cf. `https://metrics.torproject.org/users.html`

Different sorts of people

Anonymity serves different interests for different user groups



Anonymity loves company...

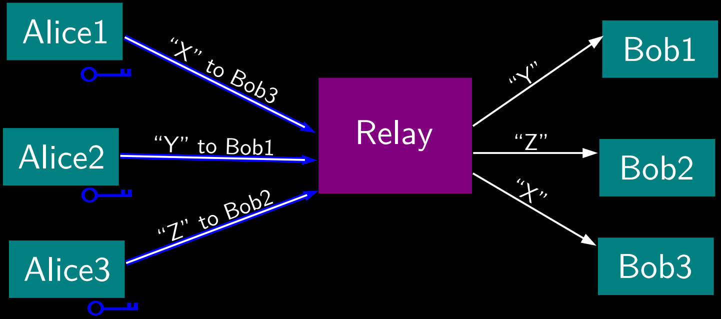
What’s Tor?

- `tor` is free software
- Running the Tor anonymity network
- Supported by *The Tor Project, Inc.*, a 501(c)(3) non-profit US organization

Onion routing

Ideas behind onion routing

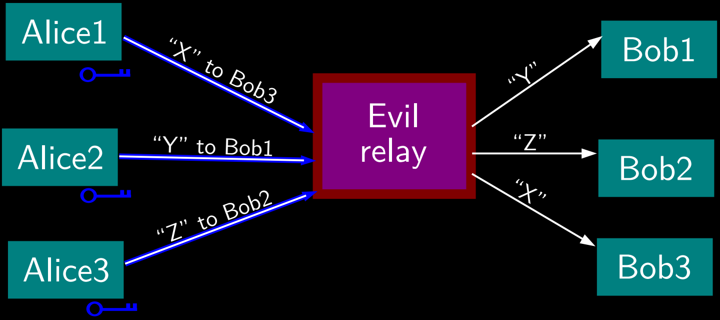
The simplest design use a single relay to hide connections



(example: some commercial proxy providers)

Ideas behind onion routing

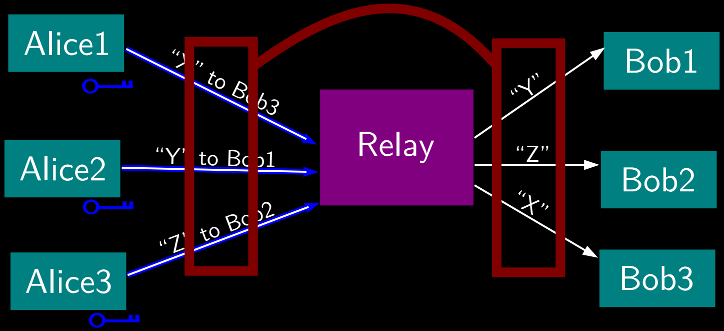
But a single relay (or eavesdropper!) is a single point of failure



Ideas behind onion routing

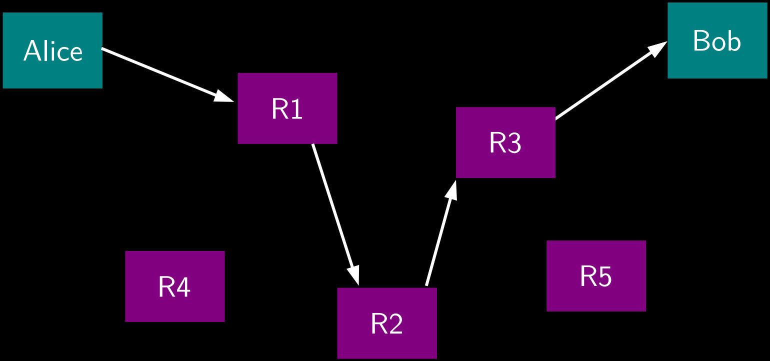
... or a single point of bypass

(timing analysis allows to match sources and destinations)



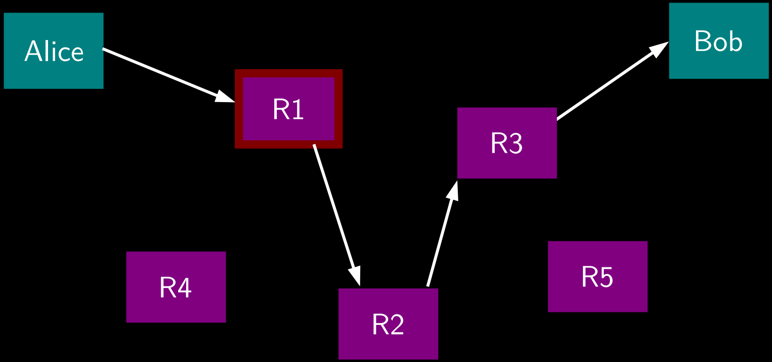
Ideas behind onion routing

So, add multiple relays so that no single one can betray Alice



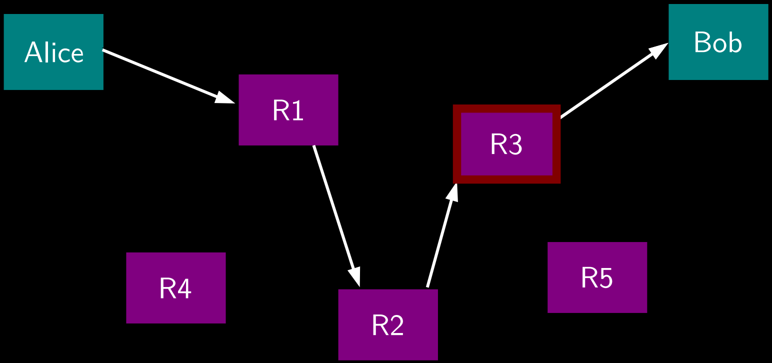
Ideas behind onion routing

A corrupt first hop can tell that Alice is talking, but not to whom



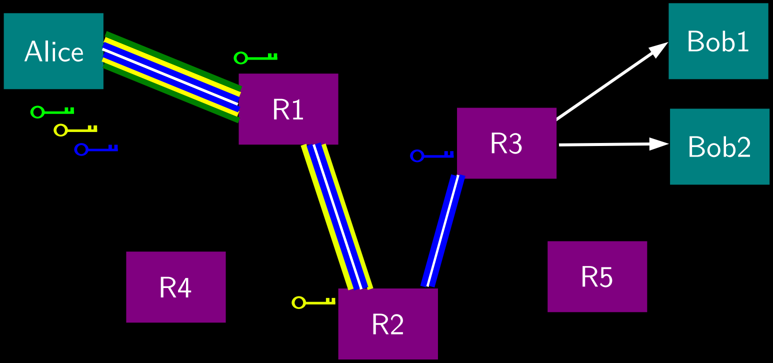
Ideas behind onion routing

A corrupt final hop can tell that somebody is talking to Bob, but not who



Ideas behind onion routing

Alice makes a session key with R1... and then tunnels to R2... and to R3

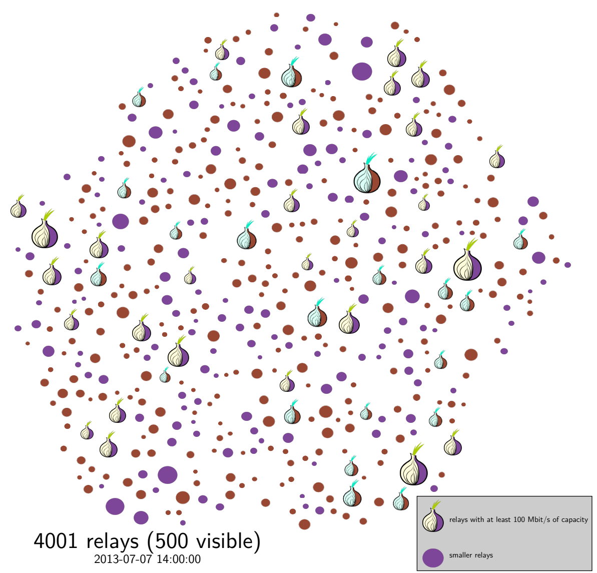


The Tor network

The Tor network

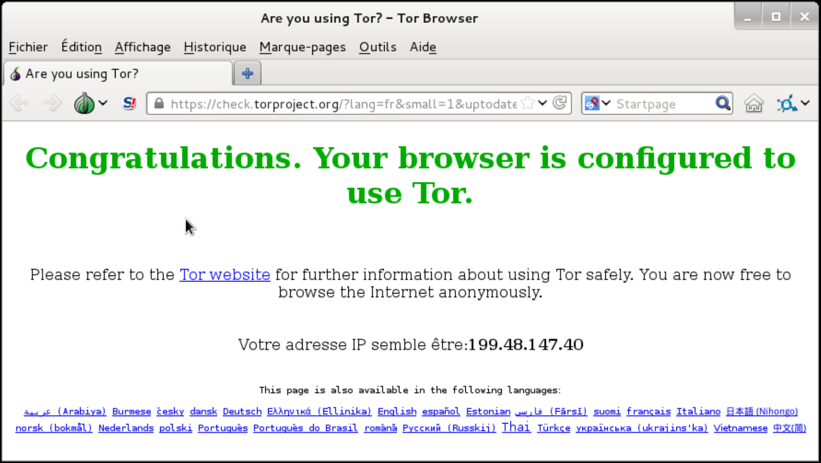
- nearly 4000 relays
- around 3600 volunteer operators
- current total measured bandwidth 35 Gb/s
- diversity issue: a mere 40 relays see 80% of the total traffic

The Tor network



Using Tor

Using Tor: the Tor Browser Bundle


Are you using Tor? – Tor Browser
Fichier
Édition
Affichage
Historique
Marque-pages
Outils
Aide
Are you using Tor?
https://check.torproject.org/?lang=fr&small=1&uptodate
Startpage

Congratulations. Your browser is configured to use Tor.

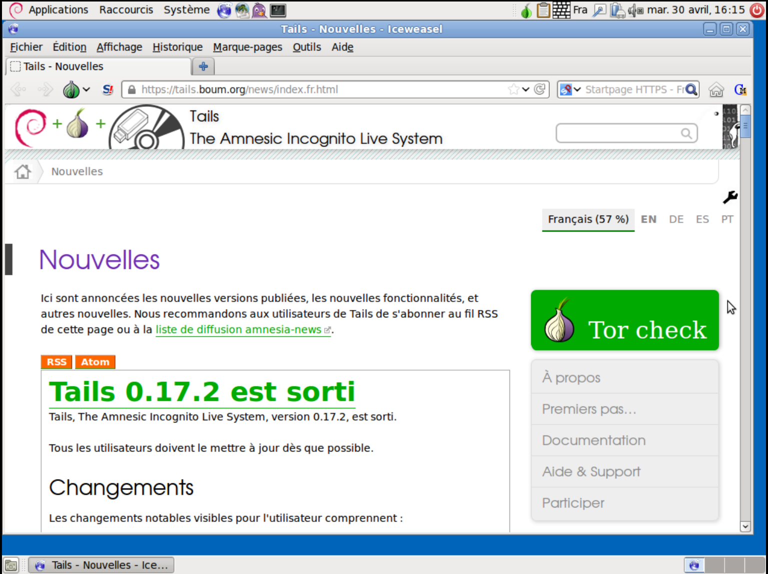
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Votre adresse IP semble être:**199.48.147.40**

This page is also available in the following languages:

عربية (Arabiya) Burmese česky dansk Deutsch Ελληνικά (Ellinika) English español Estonian فارسی (Fārsī) suomi français Italiano 日本語 (Nihongo) norsk (bokmål) Nederlands polski Português Português do Brasil română Русский (Russkij) Thai Türkçe українська (ukrajins'ka) Vietnamese 中文(简)

Using Tor: the Tails live system



Applications Raccourcis Système
Fra mar. 30 avril, 16:15
Tails - Nouvelles - Iceweasel
Fichier Édition Affichage Historique Marque-pages Outils Aide
Tails - Nouvelles
https://tails.boum.org/news/index.fr.html
Startpage HTTPS - Fr
Tails - Nouvelles - Ice…

Tails
The Amnesic Incognito Live System

Nouvelles

Français (57 %) EN DE ES PT

Nouvelles

Ici sont annoncées les nouvelles versions publiées, les nouvelles fonctionnalités, et autres nouvelles. Nous recommandons aux utilisateurs de Tails de s'abonner au fil RSS de cette page ou à la liste de diffusion amnesia-news.

RSS Atom

Tails 0.17.2 est sorti

Tails, The Amnesic Incognito Live System, version 0.17.2, est sorti.

Tous les utilisateurs doivent le mettre à jour dès que possible.

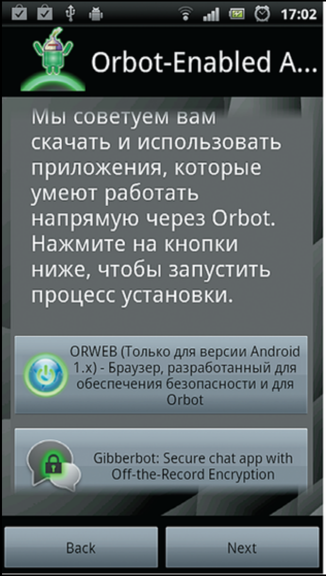
Changements

Les changements notables visibles pour l'utilisateur comprennent :

Tor check

- À propos
- Premiers pas…
- Documentation
- Aide & Support
- Participer

Using Tor: Orbot and Orweb



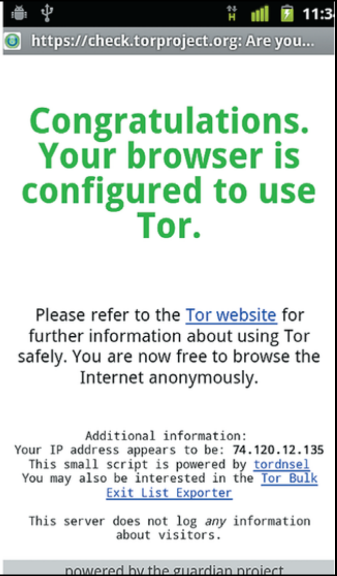
17:02

Orbot-Enabled A...

Мы советуем вам скачать и использовать приложения, которые умеют работать напрямую через Orbot. Нажмите на кнопки ниже, чтобы запустить процесс установки.

ORWEB (Только для версии Android 1.x) - Браузер, разработанный для обеспечения безопасности и для Orbot

Gibberbot: Secure chat app with Off-the-Record Encryption



11:3

https://check.torproject.org: Are you...

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

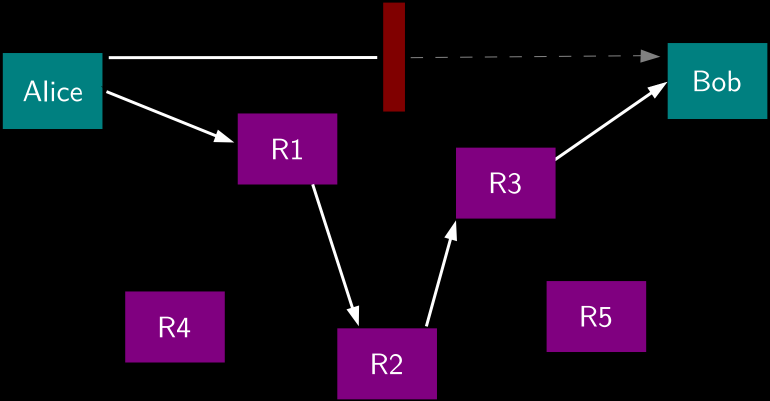
Additional information:
Your IP address appears to be: 74.120.12.135
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log *any* information about visitors.

powered by the guardian project

Circumventing censorship

Tor helps circumventing censorship



Tor routes around censorship

Censors do not want Tor

- The list of Tor relays is public
- Upside: server administrators can block exit nodes if they really need to
- Downside: allow blocking access to the Tor network

Direct Tor connections are currently blocked in China, Iran, Kazakhstan, Syria, the Philippines, …

Bridges

- Limited kind of Tor relay
- Private entry point in the Tor network
- Different pool of bridge addresses
- Some bridges are completely private

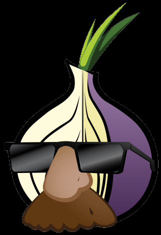
But the arm race goes on...

Censors really do not want Tor

- Tor traffic is recognizable
- Deep Packet Inspection became pervasive

Obfuscated bridges

- `obfsproxy` makes traffic to a bridge looks like random noise
- *Pluggable* transport framework to enable research



But the arm race goes on...

Further developments

Shared secret against active probing

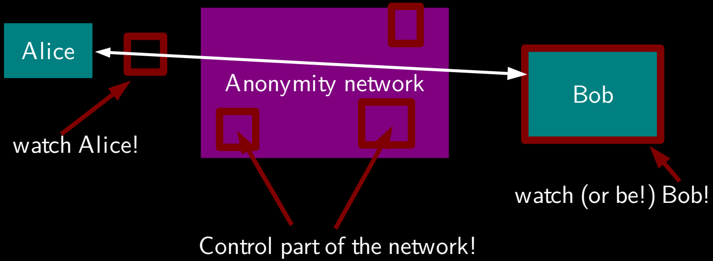
New obfuscation protocols:

- Flashproxy
- Scramblesuit
- Format Transforming Encryption
- More?

Tor is not magic

Tor does not solve all problems

Threat model:
what can the attacker do?



Case study

- I present you Wendy.

Case study

- I present you Wendy.
- Wendy works at ACME, Corp.

Case study

- I present you Wendy.
- Wendy works at ACME, Corp.
- She discovers that ACME is releasing toxic waste in the environment.

Case study

- I present you Wendy.
- Wendy works at ACME, Corp.
- She discovers that ACME is releasing toxic waste in the environment.
- **She wants the word out.**

Case study

Case study

How to **hide who**'s blowing the whistle?

Case study

In order to **publish pictures and other documents** about the issue:

- Create a blog on a free service.
- Always connected using Tor.

Pros: provider is unable to tell Wendy's location

Cons: provider might shut down the blog in case of troubles

Case study

Should Wendy work on her blog at **work**?

- Tor traffic might stand out
- `obfsproxyssh` could do the trick, but not integrated yet

Case study

Should Wendy work on her blog at **home**?

Watch out for traffic confirmation attacks!

Case study

- Few people can possibly know about this
- Tor is a low-latency network
- Monitoring Wi-Fi requires nothing more than being at range
- Packet flow can match the pattern of publishing a blog post

Case study

Make traffic confirmation attacks harder:

- Blur the local traffic by participating in torrents
- Blur the remote traffic by uploading unrelated files to the blog provider
- Set a publication date so the blog post does not appear immediately after

Case study

Another option would be to get a journalist to write about the story.

But we need to train journalists in secure communications!

Case study

What if her computer gets **searched** or **attacked by a malware** planted by the company?

Use Tails:

- No traces on her computers
- Live systems are a lot harder to compromise

Case study

Yet another pitfall: **metadata**.

Digital cameras embed date, time, serial numbers and other information in picture file.

Tails ships with the *Metadata Anonymization Toolkit* which can easily remove them.

Case study

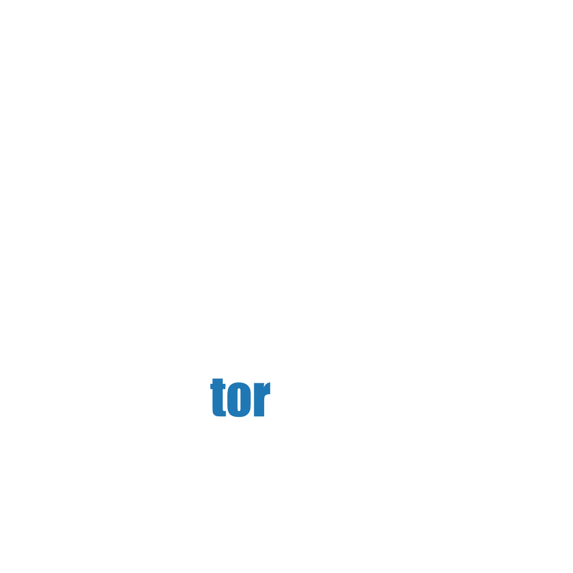
Summary of a possible solution:

- Always use Tails
- Strip metadata using MAT
- Publish on a blog on a free platform
- Articles can be prepared at home
- The blog takes care of publishing the article at a later time

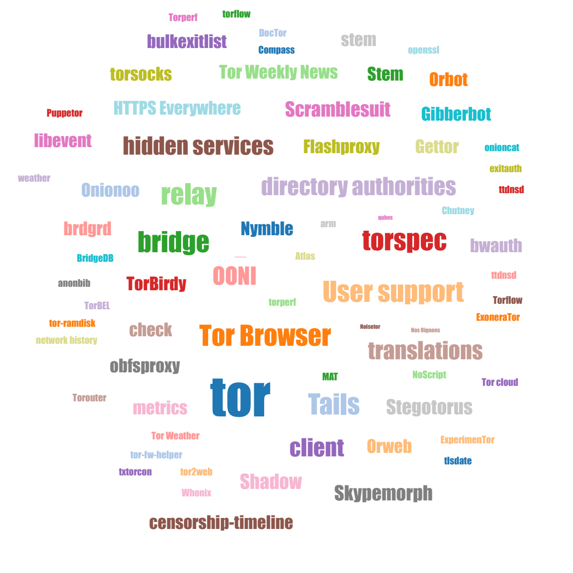
Wendy should try to imitate someone else writing style to resist stylometry analysis.

Want to help?

The Tor ecosystem



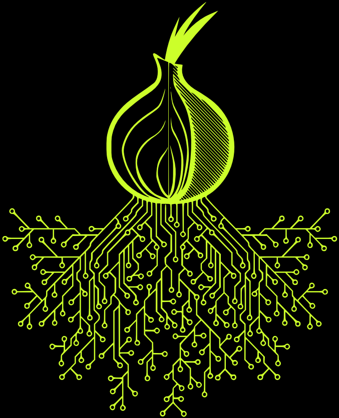
The Tor ecosystem



Help is more than welcome!

- Support
- Translations
- Development (C, Python, C++, JavaScript, Java, …)
- Research
- Testing
- Documentation
- Outreach
- Financial support

Questions?



- English support: `help@rt.torproject.org`
- French support: `help-fr@rt.torproject.org`
- Press requests: `execdir@toproject.org`