



Anonymity On The Web

Francesco Locatello
Michael König ETH Zürich

April 29, 2015

Fact:



We are being watched.

Who needs anonymity?

Who needs anonymity?



Who needs anonymity?

Normal people:

- Identity thieves

Who needs anonymity?

Normal people:

- Identity thieves
- Irresponsible corporations

Who needs anonymity?

Normal people:

- Identity thieves
- Irresponsible corporations
- Sensitive topics

Who needs anonymity?

Normal people:

- Identity thieves
- Irresponsible corporations
- Sensitive topics
- Circumvent censorship

How to retain it?



How to retain it?



Tor mission:

"Tor aims to provide protection for ordinary people who want to follow the law."

What to do with Tor:

What to do with Tor:

Access web sites anonymously

What to do with Tor:

Access web sites anonymously

Host web servers with anonymous location

Tor in real life

Tor in real life

Torbook

Login ID: Password:

Keep me logged in [Forgot your password?](#)

Sign Up
It's free and always will be.

*Full Name:

*Email:

*Password:

Captcha Challenge

Type in the verification code above

Torbook helps you connect and share with the people in your life.

03:26 p.m.
04/03/2014

Tor in real life



Silk Road
anonymous market

messages 0 | orders 0 | account \$0.00

Search

Go

Shop by Category

Drugs 8,670

Cannabis 2,066

Dissociatives 165

Ecstasy 660

Opioids 591

Other 455

Precursors 50

Prescription 2,146

Psychedelics 981

Stimulants 1,102

Apparel 264

Art 127

Biotic materials 1

Books 861

Collectibles 5

Computer equipment 32

Custom Orders 68

Digital goods 509

Drug paraphernalia 305

Electronics 77



1g MDMA 82%+ High
Quality -Made in Germany-
\$1.30



50 gr. Crystal MDMA Rocks
\$23.33



Valium 10mg/ Diazepam
(100 Pills)
\$2.32



3g Xxx AAA QUALITY
WEED,AMAZING
\$0.98



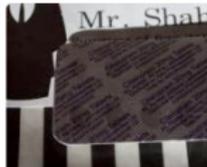
[Kamagra jelly \(India\), 1
week pack](#)
\$0.98



Honeycomb Wax (85+%
THC) Fully Purged
\$1.45



1 gram * Moroccan Hash *
DUTCH QUALITY
\$0.27



Citalopram 10x 20mg table
\$0.10

Anonymity On The Web



Anonymity On The Web



Definition:

Allow users to communicate privately by hiding their identities from the recipient or third parties on the internet.

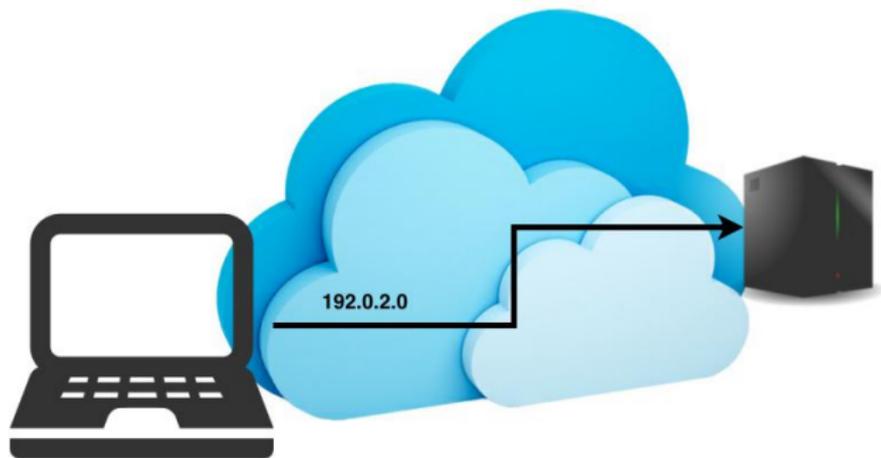
A web perspective

A web perspective



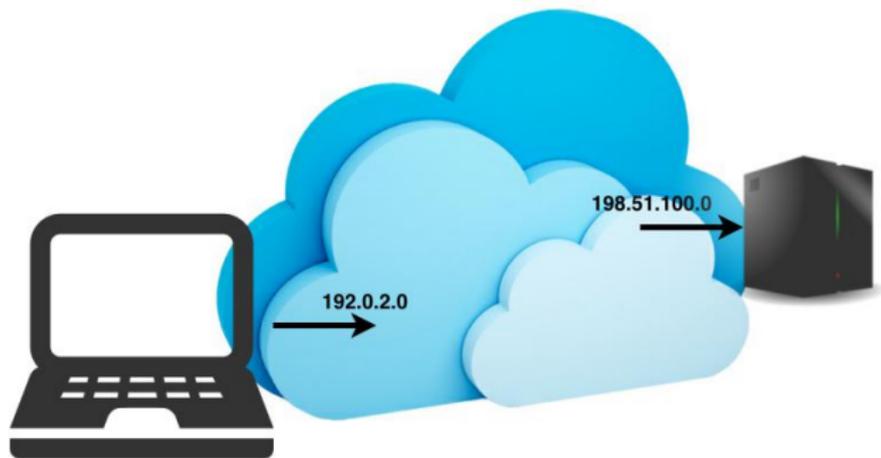
The web cloud

A web prospective



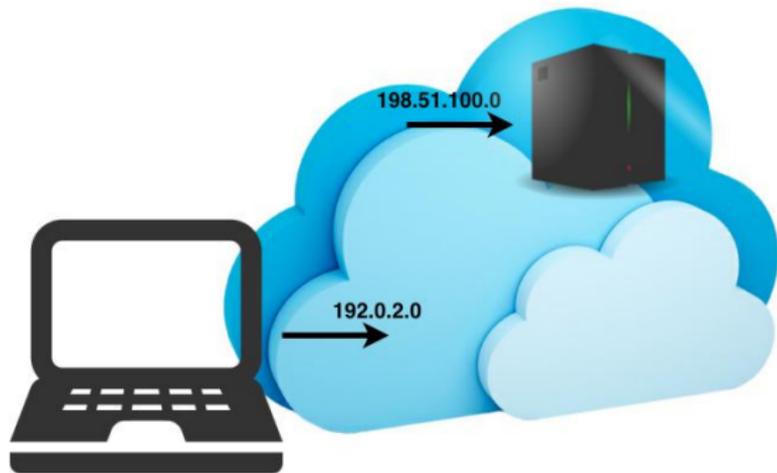
Direct connection

A web prospective



Tor breaks this link

A web perspective



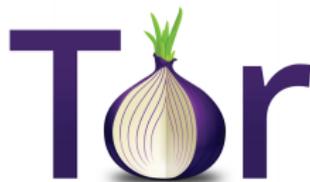
Host website anonymously: no registered domain name, no hosting account

Outline

- 1 Tor
 - Structure
 - Strengths
 - Weaknesses
- 2 Dissent
 - Foundations of Anonymity
- 3 Conclusion

How to use Tor:

Download the Tor client also called Onion proxy

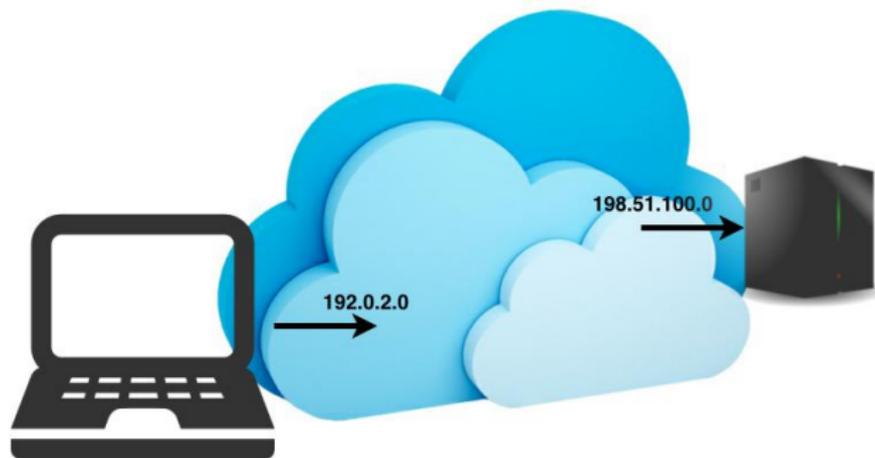


How to use Tor:

Download the Tor client also called Onion proxy

What does Tor do for you:

Tor protects the transport of data, it doesn't hide user informations (Tor browser).



Getting started with anonymity

Getting started with anonymity



Getting started with anonymity



Getting started with anonymity



Getting started with anonymity



Proxy

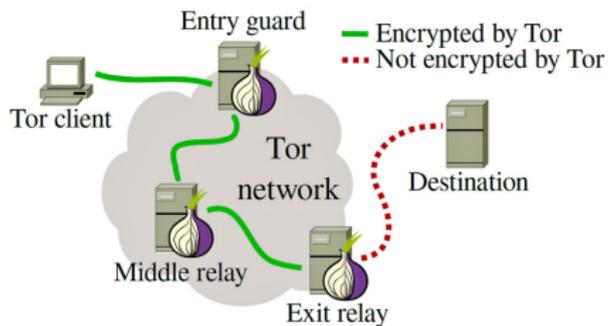


Proxy

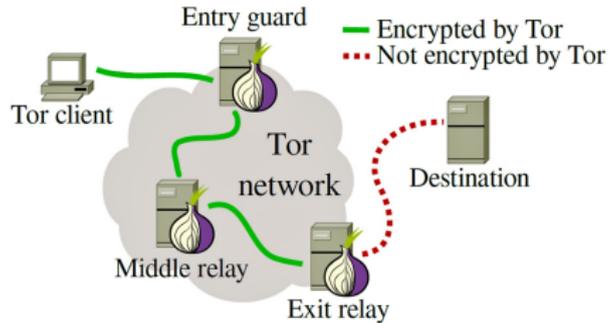


Do you trust the proxy?

The topology of the Tor Network

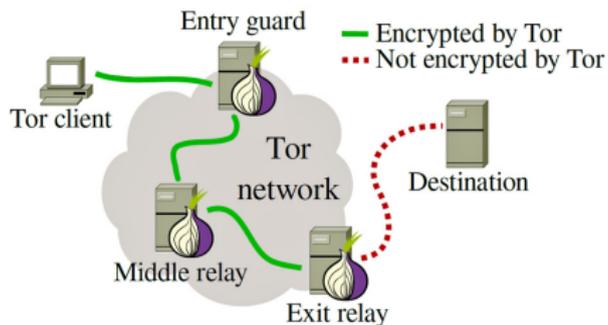


The topology of the Tor Network



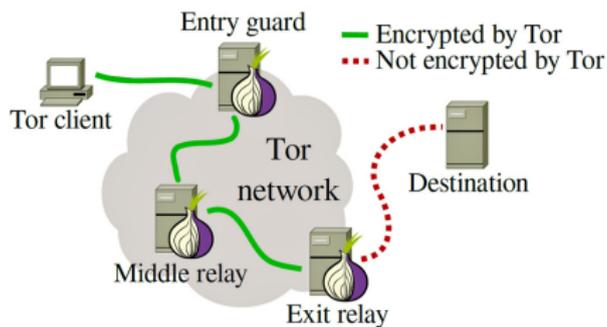
- Ran by volunteers all over the world

The topology of the Tor Network



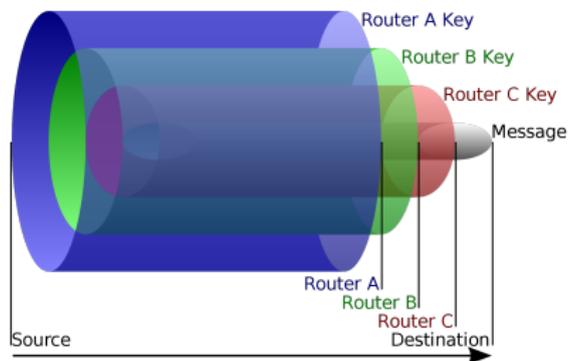
- Ran by volunteers all over the world
- Learning what sites you visit

The topology of the Tor Network

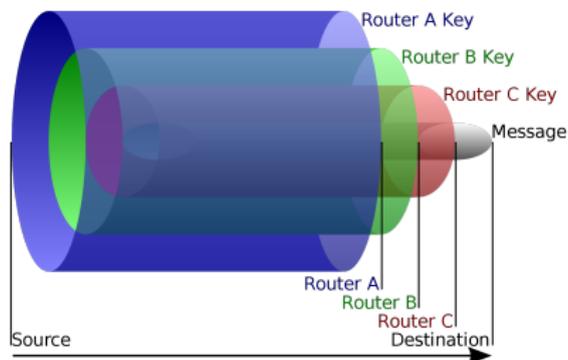
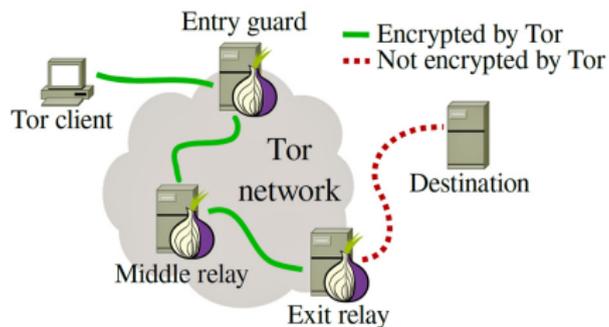


- Ran by volunteers all over the world
- Learning what sites you visit
- Learning your location

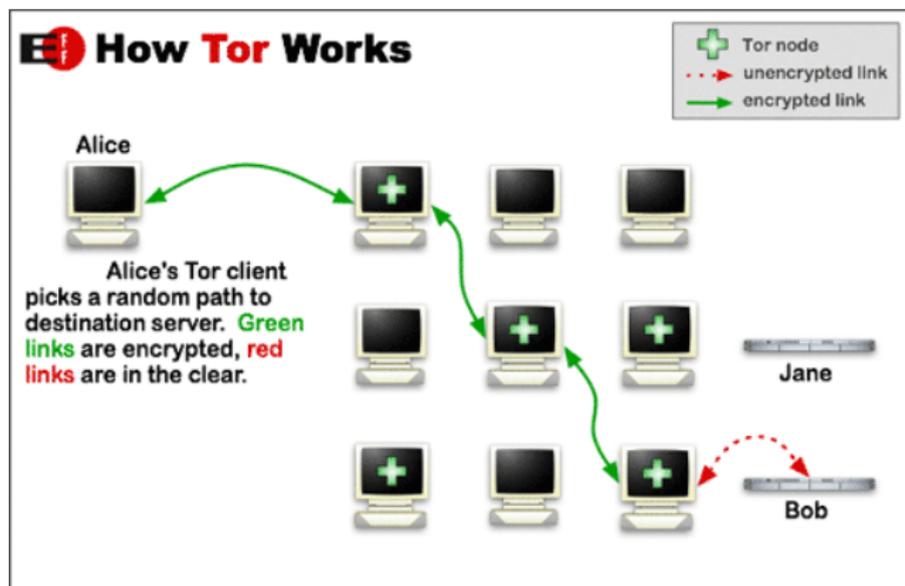
The Onion Routing



The Onion Routing

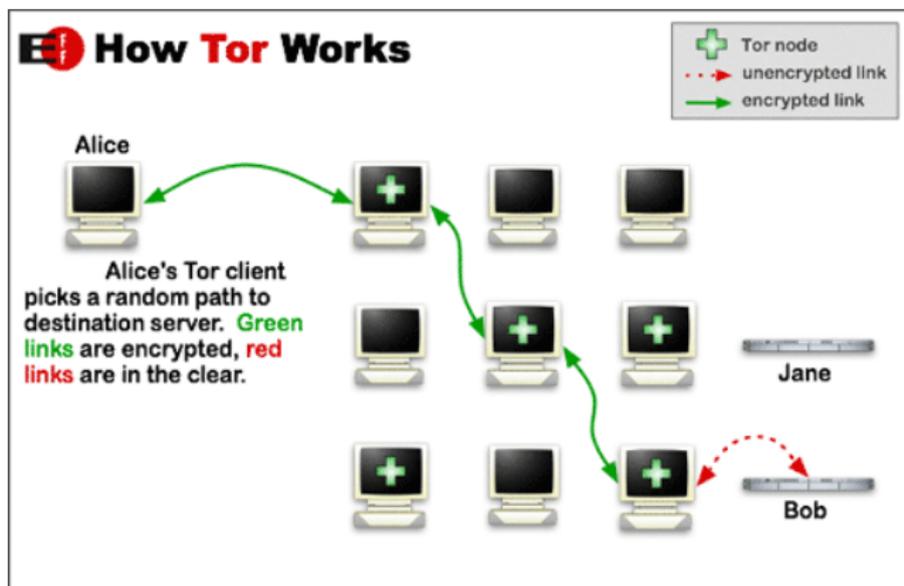


Connection Scheme



Performance: Latency and Bandwidth

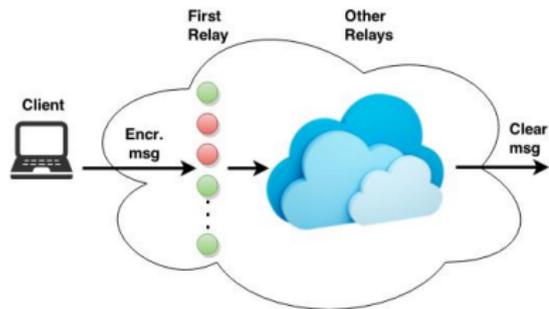
Performance: Latency and Bandwidth



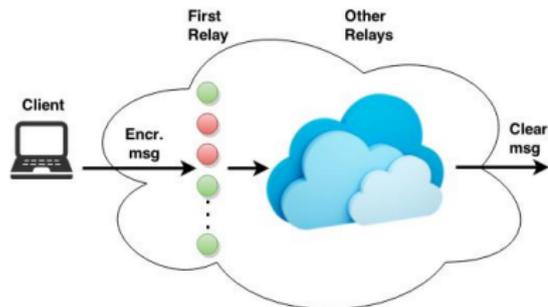
Possible Attacks:

- Side channel analysis introduction
 - Global traffic analysis (1)
 - Active attack: congestion (2)
- Intersection attack (3)
- Software exploitation and self identification (4)

See both sides of a communication channel



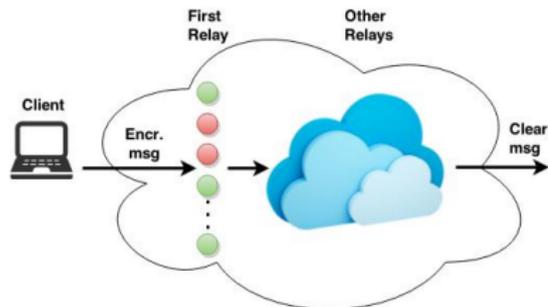
See both sides of a communication channel



$c = \#$ of controlled relays

$n = \#$ of relays

See both sides of a communication channel



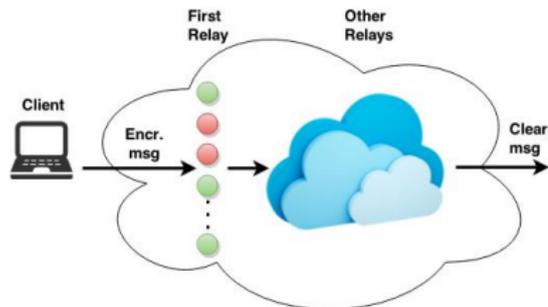
$c = \#$ of controlled relays

$n = \#$ of relays



correlation of traffic with $p = ???$

See both sides of a communication channel



$c = \#$ of controlled relays

$n = \#$ of relays



correlation of traffic with $p = \frac{c}{n}$

Side Traffic Attack

Execution Analysis

- Break cryptography

Side Traffic Attack

Execution Analysis

- Break cryptography

Traffic Analysis

- Correlate time and size of packets

Side Traffic Attack

Execution Analysis

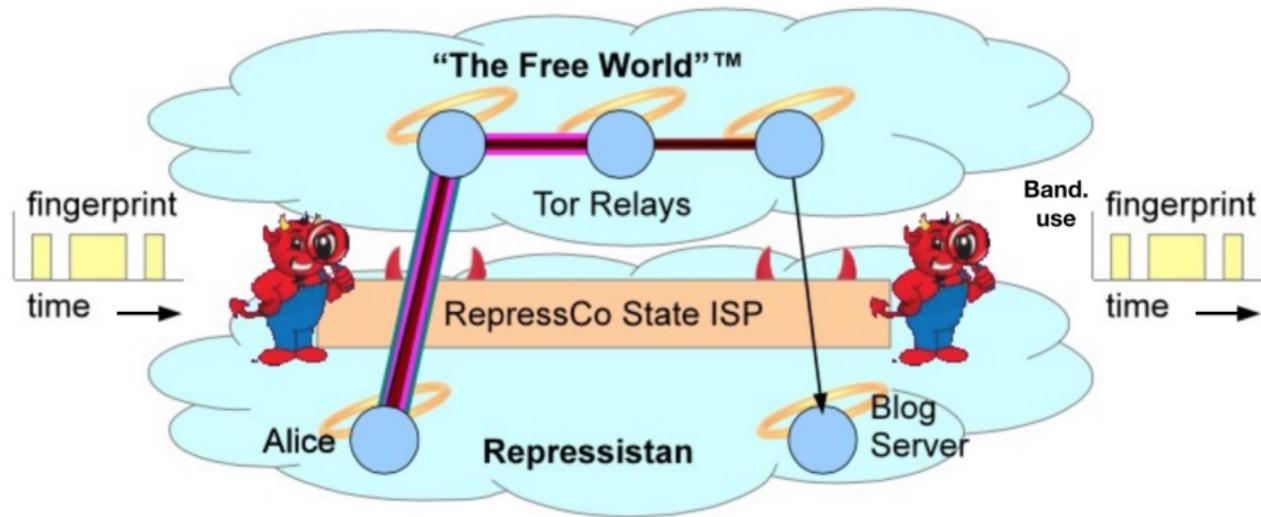
- Break cryptography

Traffic Analysis

- Correlate time and size of packets
- Deduce the path through the network

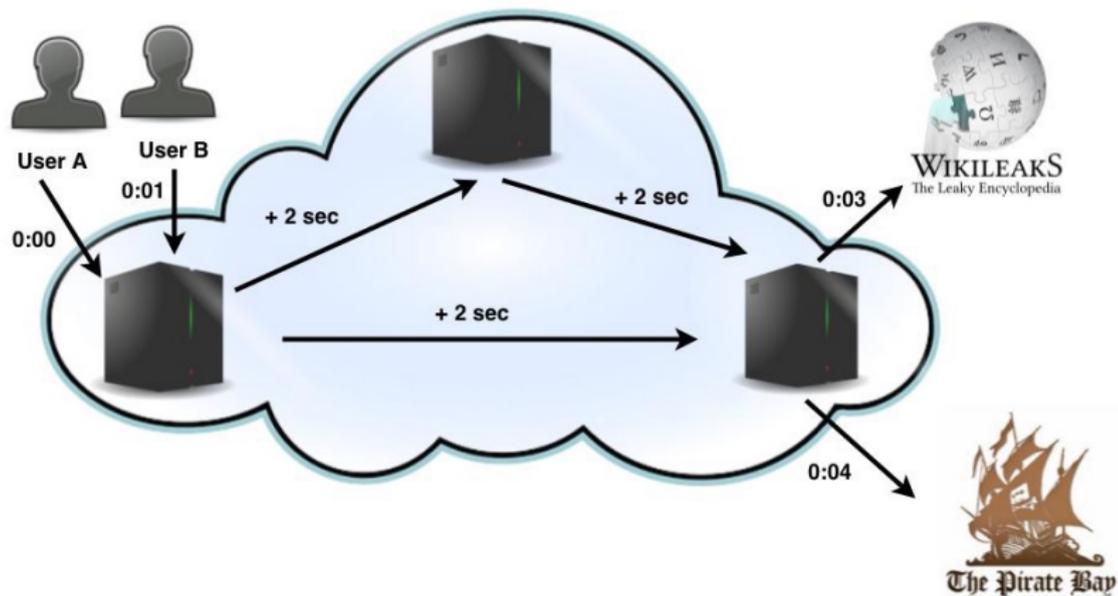
Global Traffic Analysis on Tor (1)

Global Traffic Analysis on Tor (1)

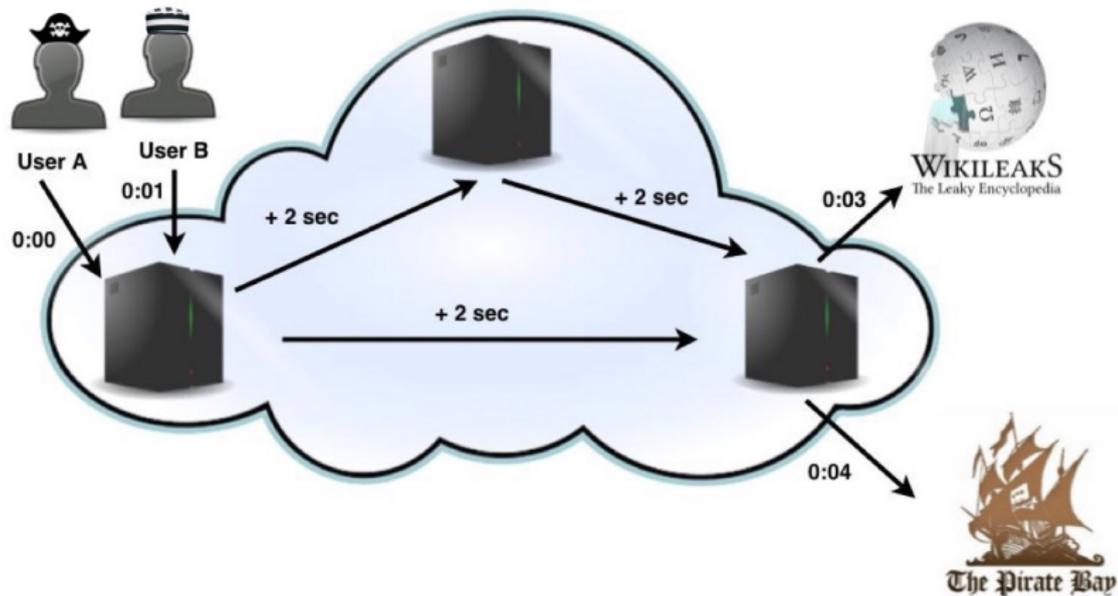


A Simple Example

A Simple Example



A Simple Example



How Tor handles it:

How Tor handles it:

Tor Network

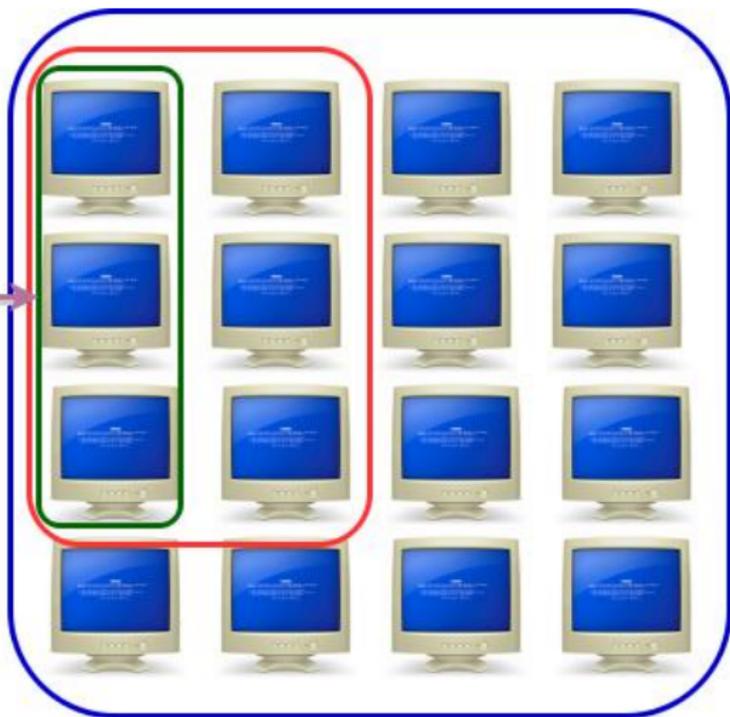
Entry Guards

Alice's Entry Guards

Alice



$P=1/3$



Why entry guards:

Why entry guards:

Those relays are not controlled
or observed

Why entry guards:

Those relays are not controlled
or observed

Those relays are observed or
controlled

Explanation: analysis over a month

Explanation: analysis over a month

Probability being safe with entry guards: $p = (1 - \frac{c}{n})^3$

Explanation: analysis over a month

Probability being safe with entry guards: $p = (1 - \frac{c}{n})^3$

Probability being safe without entry guards:

$$p_{\text{all safe}} = p_{\text{safe}}^{\text{number of connections}} = 0$$

for number of connection sufficiently big.

Active Attack: Congestion (2)

Active Attack: Congestion (2)

Assumptions:

Active Attack: Congestion (2)

Assumptions:

The attacker can either be "in the network" or own or have compromised a web server

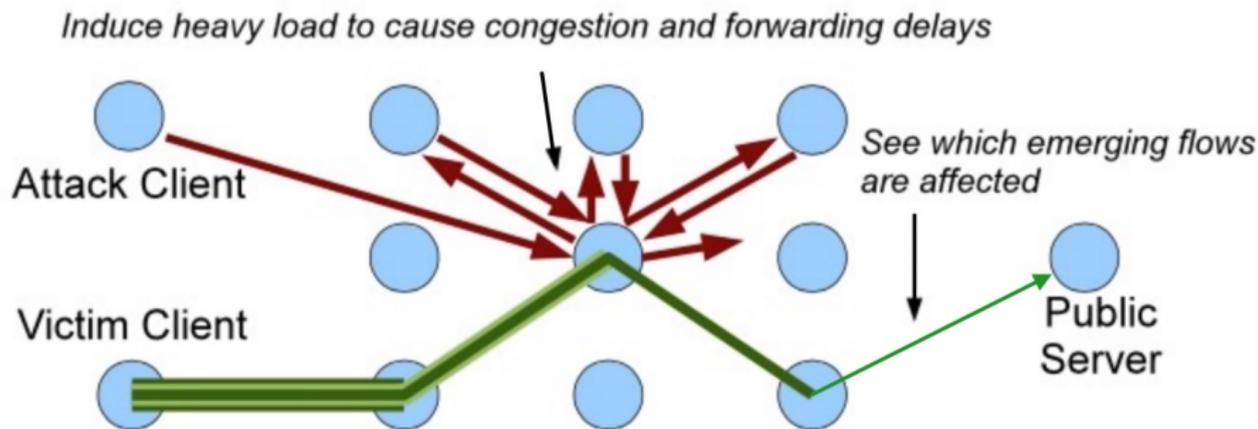
Active Attack: Congestion (2)

Assumptions:

The attacker can either be "in the network" or own or have compromised a web server

The attacker wishes to determine the set of relays through which a **long lived circuit** owned by a particular user passes (SSH).

Strategy

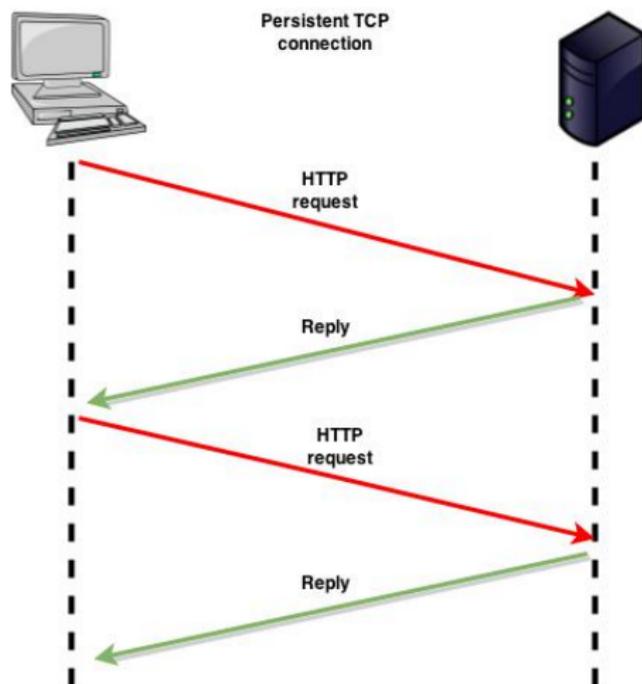


Intersection Attack: framework (3)

Intersection Attack: framework (3)

One time interaction are rare

Intersection Attack: framework (3)



Intersection Attack: framework (3)

The image shows the homepage of the TorGuard website. At the top left is the TorGuard logo with the tagline "Online Privacy Protection Services". A navigation bar contains links for "Home", "Torrent Proxy", "Anonymous VPN", "More Info...", "Members Area", and "Setup Guides". The main banner features the text "Anonymous Email Service" and "Secure G/PGP Encrypted Webmail" in large, bold letters. To the right of the banner is a diagram showing various devices (laptop, smartphone, tablet, router) connected to a central cloud icon with a keyhole, representing secure communication. Below the banner, a section titled "Secure your email from prying eyes" compares the state "Before" (with icons of envelopes and a network diagram) and "After" (with a screenshot of an email header showing "TorGuard [encrypted webmail]" and "end-to-end encryption").

TorGuard
Online Privacy Protection Services

Home | Torrent Proxy | Anonymous VPN | More Info... | Members Area | Setup Guides

Anonymous Email Service

Secure G/PGP Encrypted Webmail

TorGuard Everything.
Protect your online identity

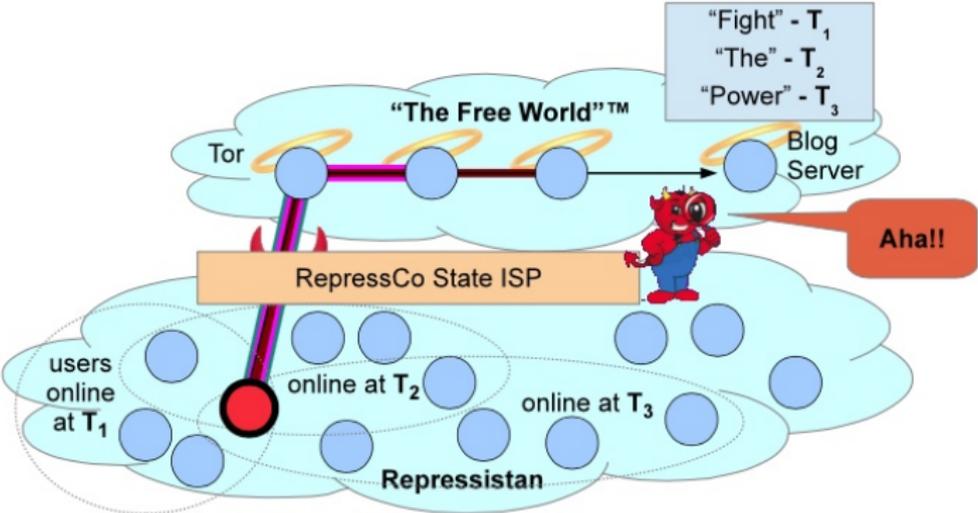
Secure your email from prying eyes

Before After

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.5 (GNU/Linux)

[Screenshot of an email header with a TorGuard logo and the text "TorGuard [encrypted webmail]" and "end-to-end encryption"]

Effectiveness





Runa A. Sandvik
Contributor

FOLLOW

*I cover all things
privacy, security
and technology.*
full bio →

Opinions expressed by Forbes
Contributors are their own.



Share

Comment
Now

TECH | 12/18/2013 @ 1:46PM | 59,109 views

Harvard Student Receives F For Tor Failure While Sending 'Anonymous' Bomb Threat

+ Comment Now + Follow Comments

On Tuesday, the FBI filed a [criminal complaint](#) against a [Harvard University](#) sophomore student for making bomb threats that led school officials to delay some final exams, including his, that had been scheduled for Monday.

According to the five-page complaint, the student “took steps to disguise his identity” by using Tor, a software which allows users to browse the web anonymously, and Guerrilla Mail, a service which allows users to create free, temporary email addresses.



(Photo credit: joeythibault)

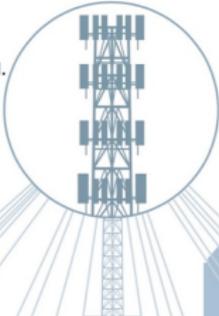
Real Life Examples

The Washington Post



Documents obtained by The Washington Post indicate that the National Security Agency is collecting billions of records a day to track the location of mobile phone users around the world. This bulk collection, performed under the NSA's international surveillance authority, taps into the telephony links of major telecommunications providers including some here in the United States.

The NSA collects this location and travel habit data to do "target development" — to find unknown associates of targets it already knows about.

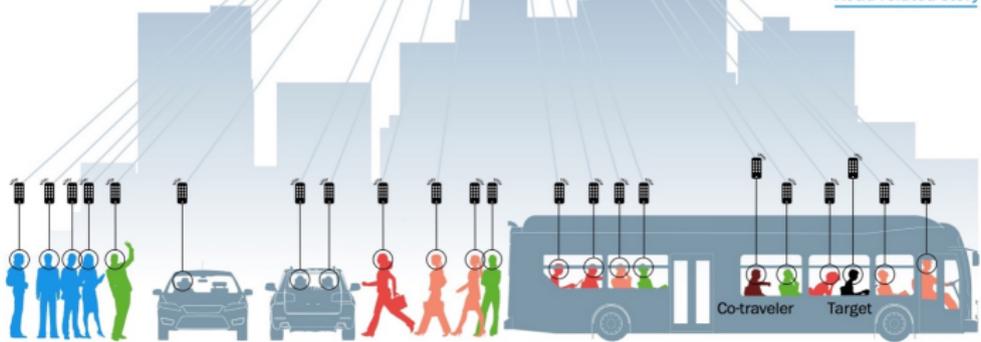


To accomplish this, the NSA compiles information on a vast database of devices and their locations. Most of those collected, by definition, are suspected of no wrongdoing. Officials say they do not purposely collect U.S. phone locations in bulk, but a large number are swept up "incidentally."

Using these vast location databases, the NSA applies sophisticated analytics techniques to identify what it calls **co-travelers** — unknown associates who might be traveling with, or meeting up with a known target.

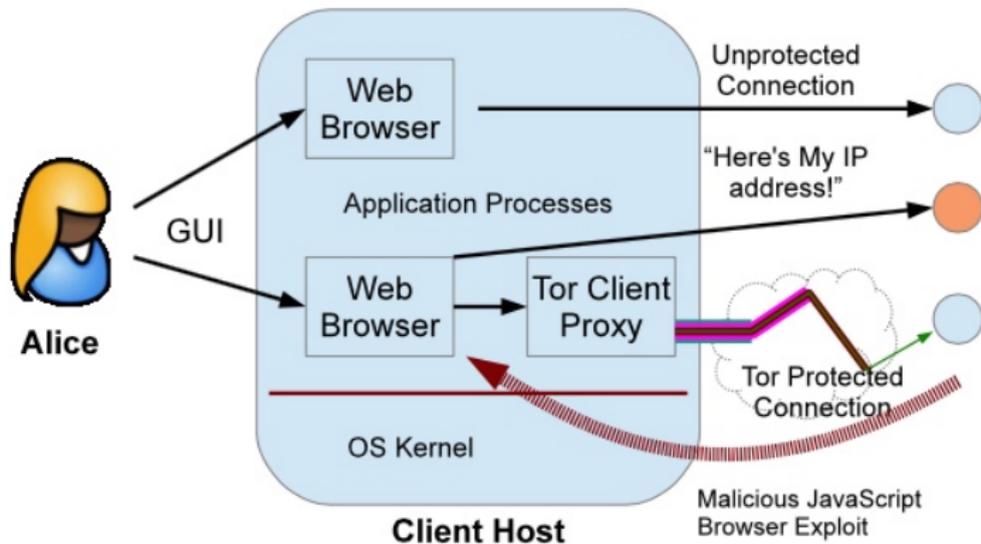
HERE IS HOW IT WORKS

[Read related story](#)



Software Exploits and Self Identification (4)

Software Exploits and Self Identification (4)



Wrap up

Attack	Tor	Dissent
Global Traffic analysis (1)		
Congestion attack (2)		
Intersection attack (3)		
Software exploits (4)		

Wrap up

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	
Congestion attack (2)	✗	
Intersection attack (3)	✗	
Software exploits (4)	✗	

Dissent: Introduction

Dissent: Introduction

The screenshot shows the GitHub web interface for the repository `DeDis / Dissent`. At the top, the GitHub logo and navigation links are visible. The repository name is prominently displayed, along with statistics: 26 watchers, 187 stars, and 26 forks. Below this, the repository description reads "Provably Anonymous Overlay" with a link to `http://dedis.cs.yale.edu/2010/anon/`. The repository statistics show 942 commits, 2 branches, 1 release, and 5 contributors. The current branch is `master`. A warning message states "use default images, not special images that we have no use for...". A list of files is shown, including `conf`, `doc`, `ext`, `src`, `utils`, `.gitignore`, `DESIGN`, `README`, `README.doxy`, `TODD`, `WEB_USE`, and `application.pro`, each with a brief description and a commit date. On the right side, there are buttons for "Code", "Issues", "Pull requests", "Pulse", and "Graphs", along with options to clone the repository or download a ZIP file.

GitHub

This repository Search Explore Features Enterprise Blog Sign up Sign in

DeDis / Dissent Watch 26 Star 187 Fork 26

Provably Anonymous Overlay <http://dedis.cs.yale.edu/2010/anon/>

942 commits 2 branches 1 release 5 contributors

branch: master Dissent / +

use default images, not special images that we have no use for...

davidhw authored on Nov 11, 2014 latest commit 84c79e838d

conf	Rewrite of the session handling code following the design	a year ago
doc	Beginnings of a Dissent use-cases document for the RATPAC	7 months ago
ext	Some initial porting to Qt5 the big remaining issues is Url parsing n...	2 years ago
src	[Application] Check keys before starting	6 months ago
utils	use default images, not special images that we have no use for...	5 months ago
.gitignore	updated gitignore	2 years ago
DESIGN	DESIGN doc update	6 months ago
README	README tweak	11 months ago
README.doxy	Doxygen / Documentation stuff	3 years ago
TODD	TODD fix	a year ago
WEB_USE	few tweaks to readme to reflect changes in config files	2 years ago
application.pro	[Web] Cleaned up WebServices	3 years ago

Code

Issues 2

Pull requests 0

Pulse

Graphs

HTTPS clone URL
<https://github.com>

You can clone with HTTPS or Subversion

Clone in Desktop

Download ZIP

Alternative foundation for anonymity:

Alternative foundation for anonymity:

- Verifiable shuffles

Alternative foundation for anonymity:

- Verifiable shuffles
- Dining cryptographers

Dissent: Introduction

Alternative foundation for anonymity:

- Verifiable shuffles
- Dining cryptographers

Framework:

Dissent: Introduction

Alternative foundation for anonymity:

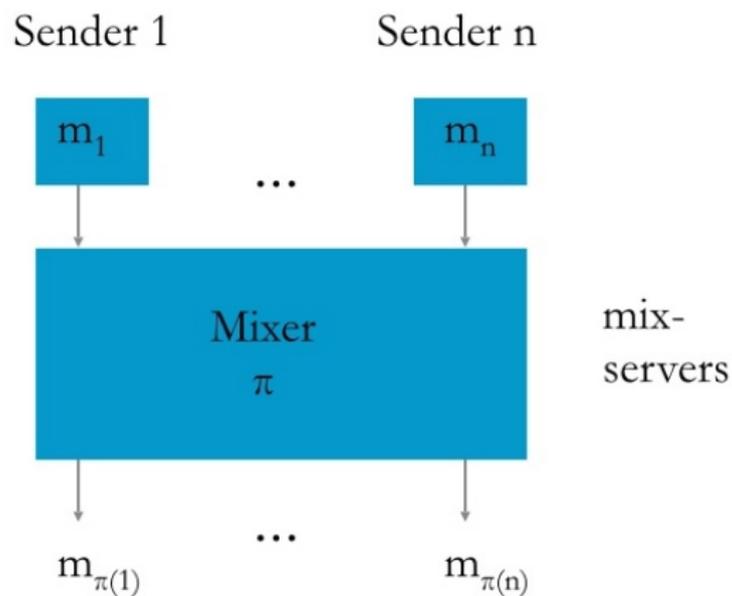
- Verifiable shuffles
- Dining cryptographers

Framework:

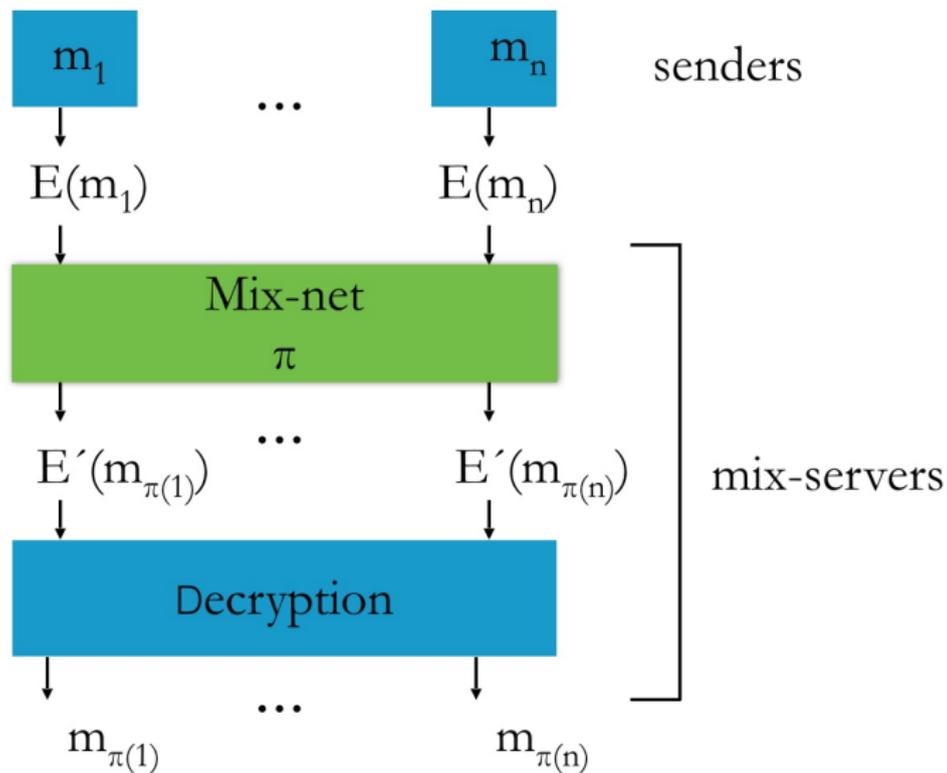
- A group of users wants to share secrets between themselves

Verifiable Shuffles: Mixing Server

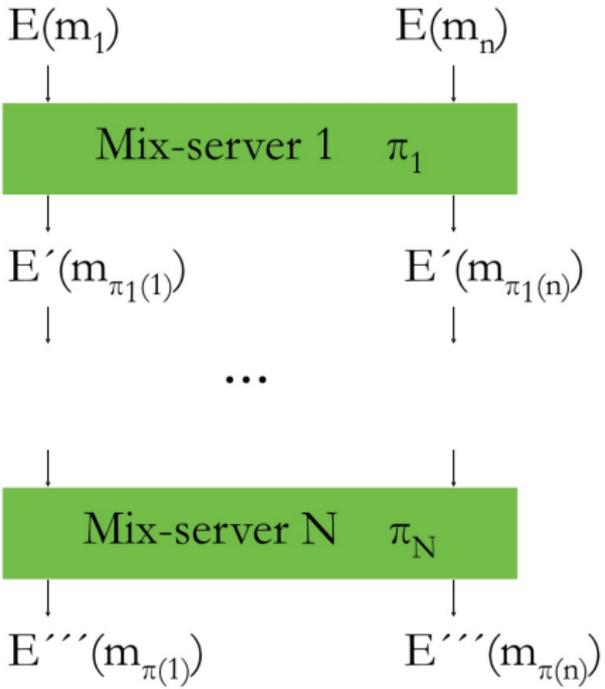
Verifiable Shuffles: Mixing Server



System Overview

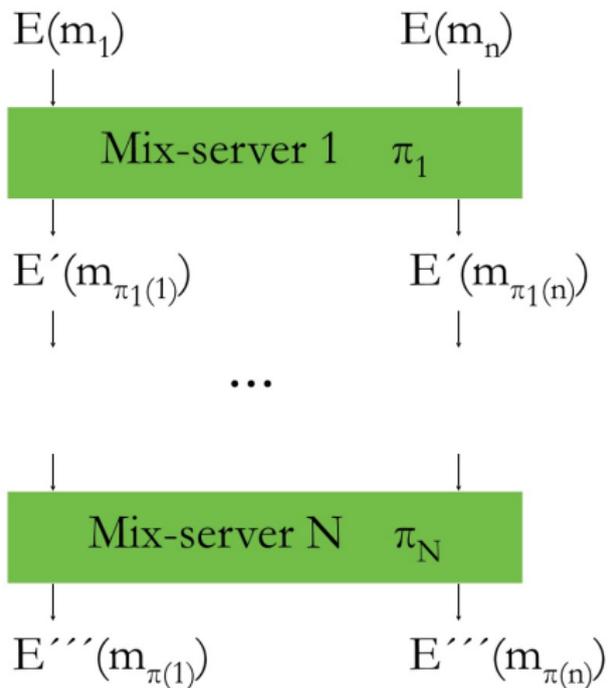


Mixing Network



$$\pi = \pi_N \circ \dots \circ \pi_1$$

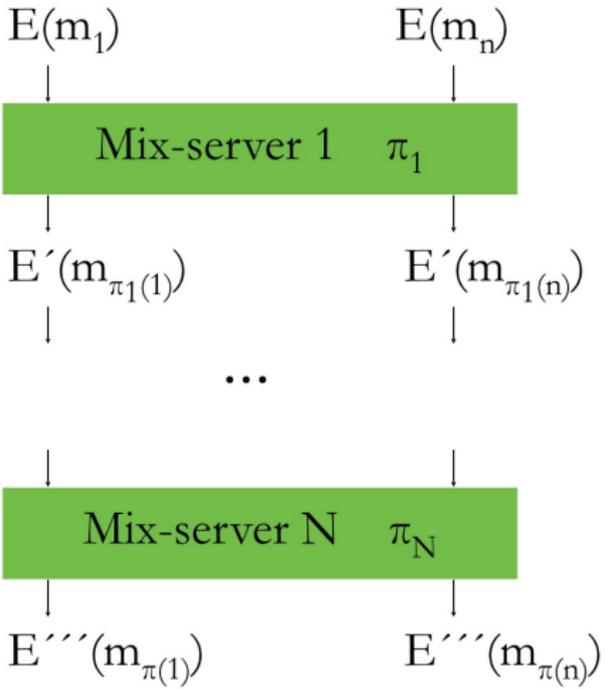
Mixing Network



- Synchronous round: concentric layers of public key encryption

$$\pi = \pi_N \circ \dots \circ \pi_1$$

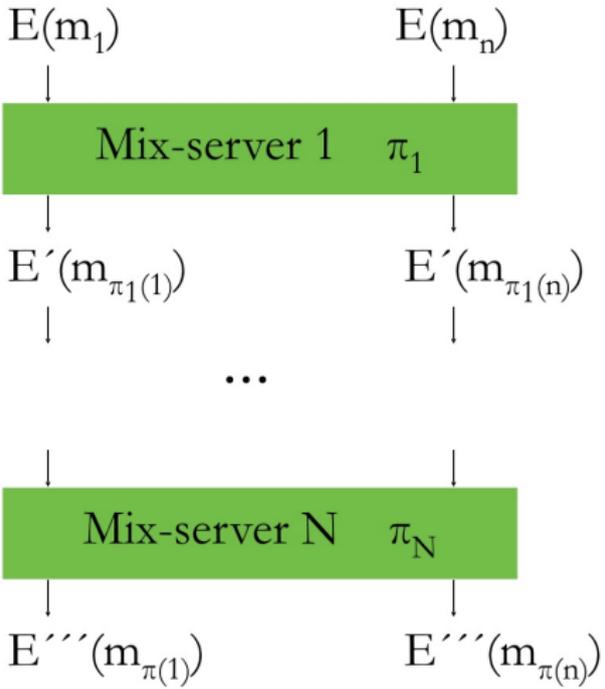
Mixing Network



- Synchronous round: concentric layers of public key encryption
- Each shuffler: unwraps, permutes and forwards

$$\pi = \pi_N \circ \dots \circ \pi_1$$

Mixing Network



- Synchronous round: concentric layers of public key encryption
- Each shuffler: unwraps, permutes and forwards
- The final shuffler: broadcasts

$$\pi = \pi_N \circ \dots \circ \pi_1$$

Considerations

Considerations

- Provable anonymity

Considerations

- Provable anonymity
- **Worst possible traffic** at each shuffler

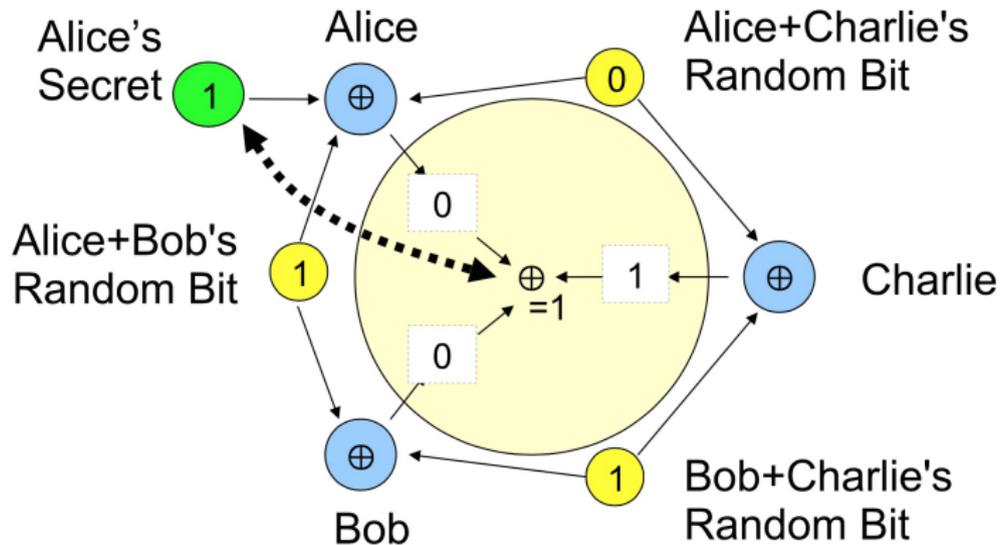
Considerations

- Provable anonymity
- **Worst possible traffic** at each shuffler
- Practical only when high latencies are tolerable

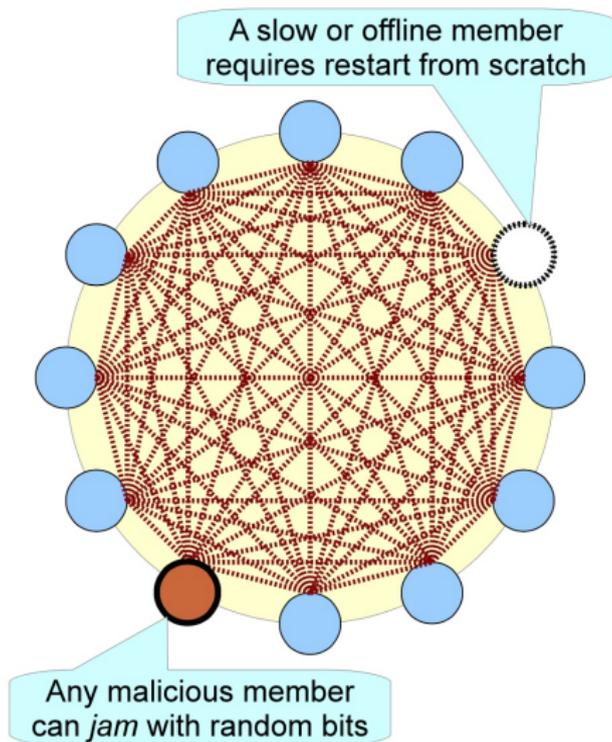
Dining cryptographers

The only well studied foundation for anonymity not based on sequential relaying is Dining Cryptographers or **DC-nets**.

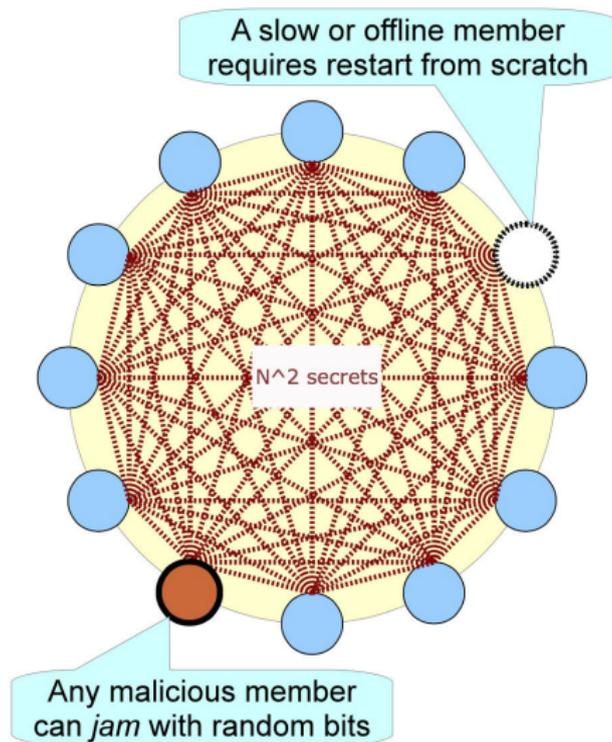
Dining cryptographers



Considerations



Considerations



Tradeoff

Weak anonymity among many nodes via onion routing

Tradeoff

Weak anonymity among many nodes via onion routing

Strong anonymity among few nodes with DC-nets

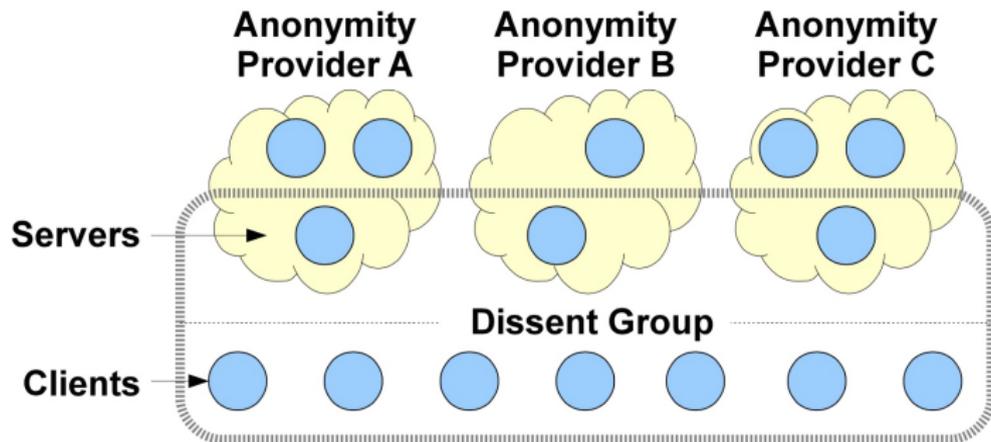
Extension

- Client/server architecture

Extension

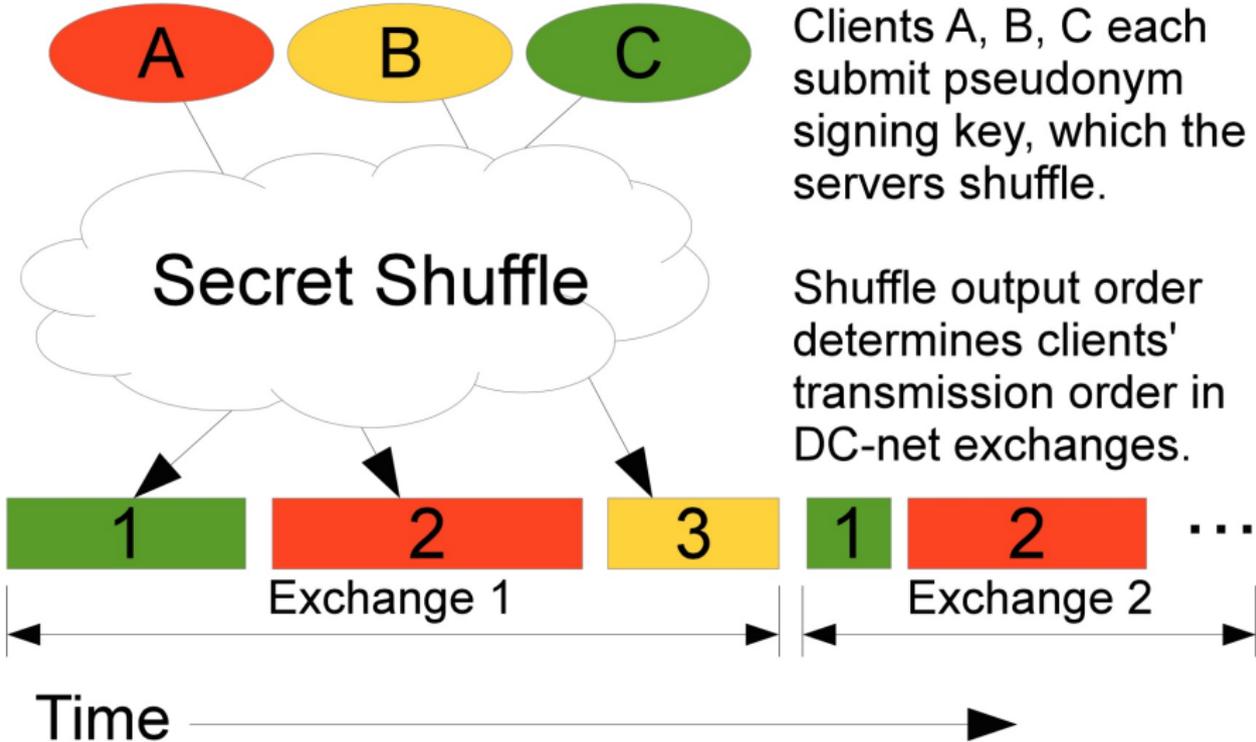
- Client/server architecture
- Clients trust only that at least one server in the set is honest, but need not know or choose which server to trust

Anytrust



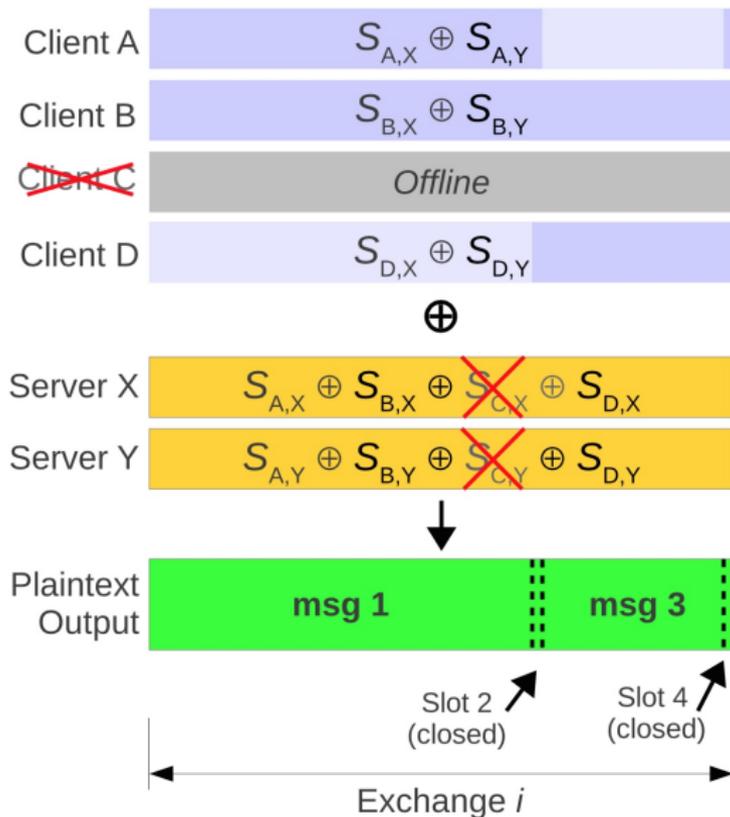
Dissent Protocol Outline Setup

Dissent Protocol Outline Setup

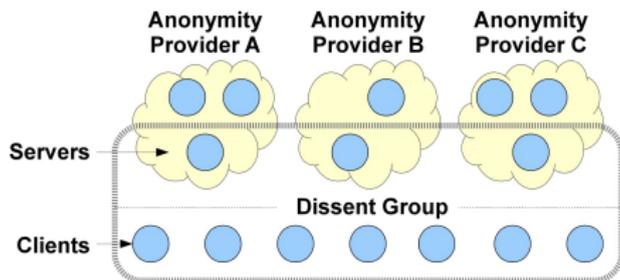


Round Structure

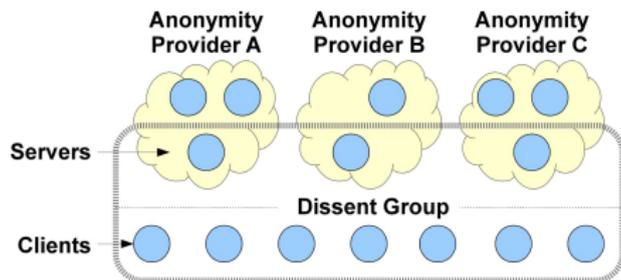
Round Structure



Scalability

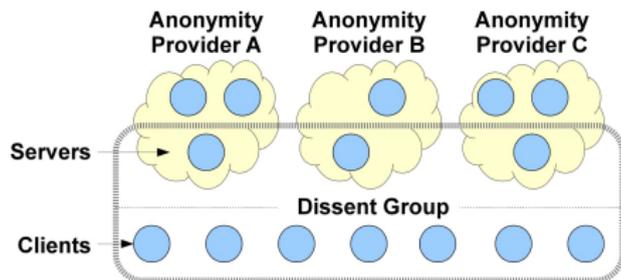


Scalability



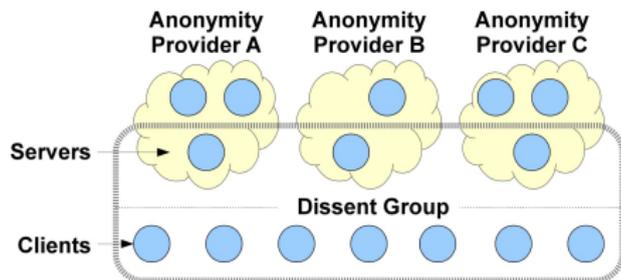
- Client: shares secrets with only $M \ll N$ servers

Scalability



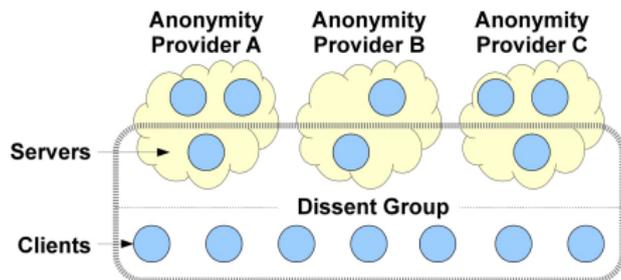
- Client: shares secrets with only $M \ll N$ servers
- Client: compute M pseudo-random bits per clear text bit

Scalability



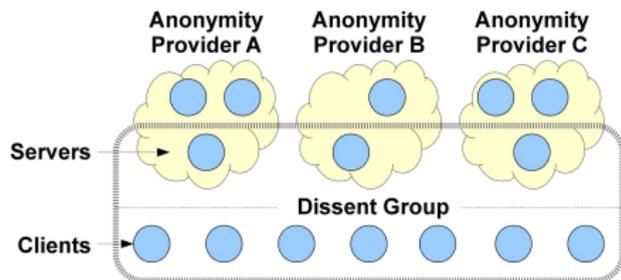
- Client: shares secrets with only $M \ll N$ servers
- Client: compute M pseudo-random bits per clear text bit
- Server: compute N pseudo-random bits per clear text bit

Scalability



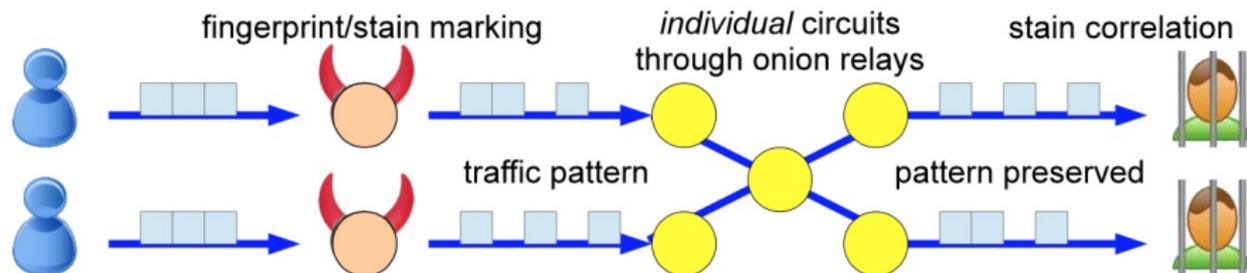
- Client: shares secrets with only $M \ll N$ servers
- Client: compute M pseudo-random bits per clear text bit
- Server: compute N pseudo-random bits per clear text bit
- Parallelizable computation

Scalability

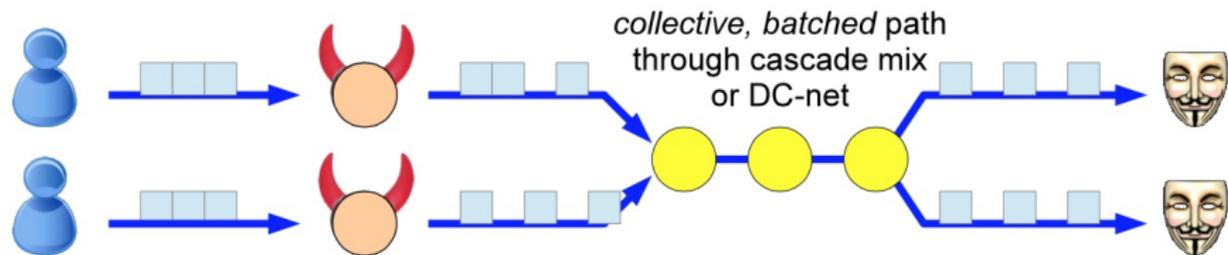


- Client: shares secrets with only $M \ll N$ servers
- Client: compute M pseudo-random bits per clear text bit
- Server: compute N pseudo-random bits per clear text bit
- Parallelizable computation
- Network churns tolerance

Handling attacks



(a) Onion routing is vulnerable to passive and active fingerprinting attacks



(b) Cascade mixes or verifiable shuffles collectively "scrub" traffic patterns

Attacks Comparison

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	
Congestion attack (2)	✗	
Intersection attack (3)	✗	
Software exploits (4)	✗	

Attacks Comparison

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	✓
Congestion attack (2)	✗	
Intersection attack (3)	✗	
Software exploits (4)	✗	

Attacks Comparison

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	✓
Congestion attack (2)	✗	✓
Intersection attack (3)	✗	
Software exploits (4)	✗	

Attacks Comparison

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	✓
Congestion attack (2)	✗	✓
Intersection attack (3)	✗	✗
Software exploits (4)	✗	

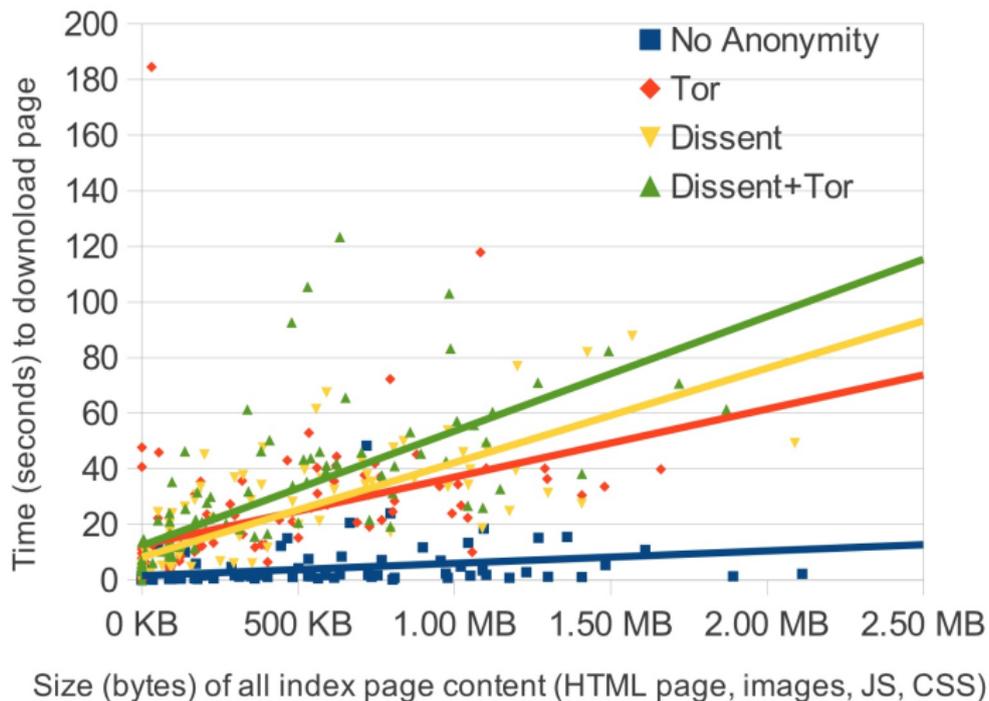
Attacks Comparison

Attack	Tor	Dissent
Global Traffic analysis (1)	✗	✓
Congestion attack (2)	✗	✓
Intersection attack (3)	✗	✗
Software exploits (4)	✗	✗

Limitations

- Scalability still limited
- Intersection attacks
- Handling server failure

Latency Considerations



Wrap up

- Latency security tradeoff for the transport of the data

Wrap up

- Latency security tradeoff for the transport of the data
 - Low latency: Tor
 - Weak anonymity guarantees

Wrap up

- Latency security tradeoff for the transport of the data
 - Low latency: Tor
 - Weak anonymity guarantees
 - Strong anonymity: Dissent
 - High latency

Conclusion

- Attacks against anonymity can be done at multiple levels

Conclusion

- Attacks against anonymity can be done at multiple levels
- There are no out of the box solutions, but....

Conclusion

- Attacks against anonymity can be done at multiple levels
- There are no out of the box solutions, but....
- There exist a set of tools that can help to provide the required level of anonymity (Tor, Tor Browser, VM, Dissent).

Questions?