

Tor OSIRIS Hack Night

Roger Dingledine, The Tor Project

March 7 2024



Tor Overview

Online anonymity: open source, open network

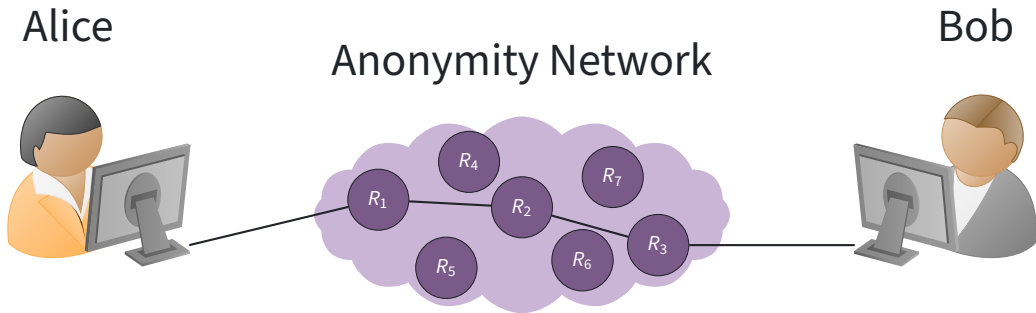
Community of devs, researchers, users, relay operators

US 501(c)(3) non-profit organization with 50ish staff

Estimated 2,000,000 to 8,000,000 daily users

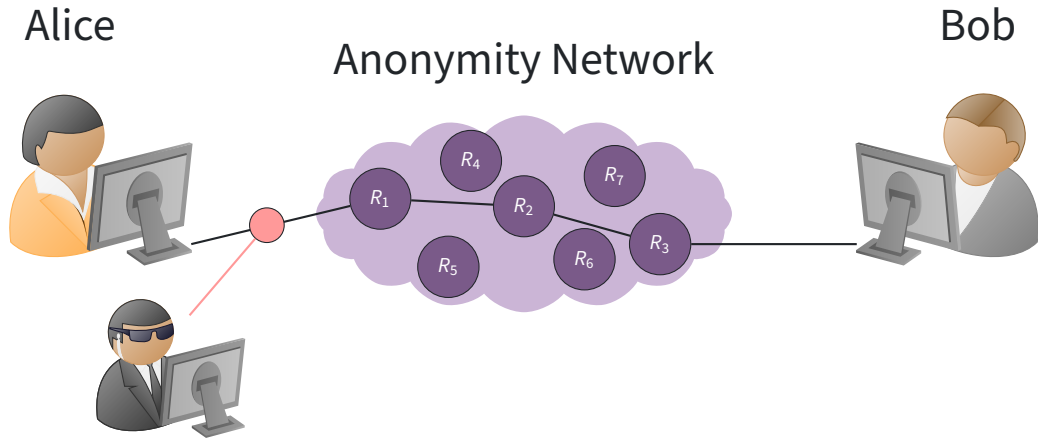
Part of larger ecosystems: internet freedom, free software, censorship resistance, anonymity research

Threat Model

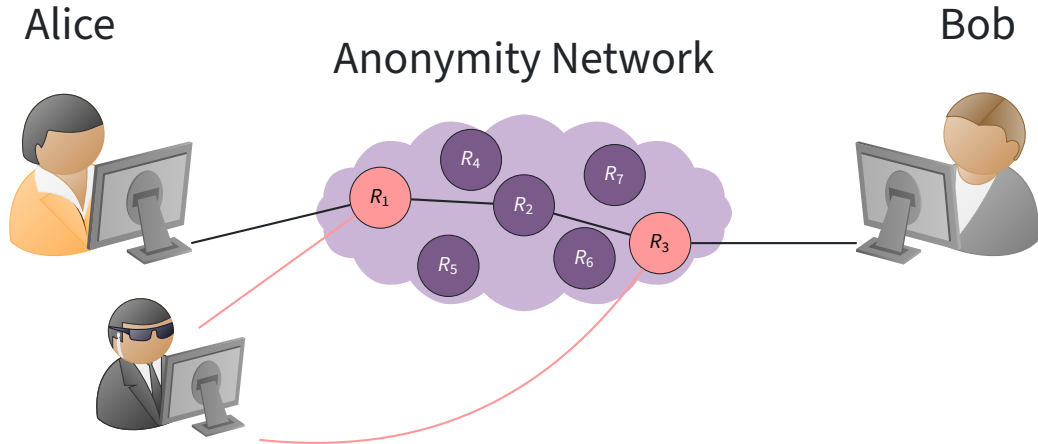


{What can the attacker do?}

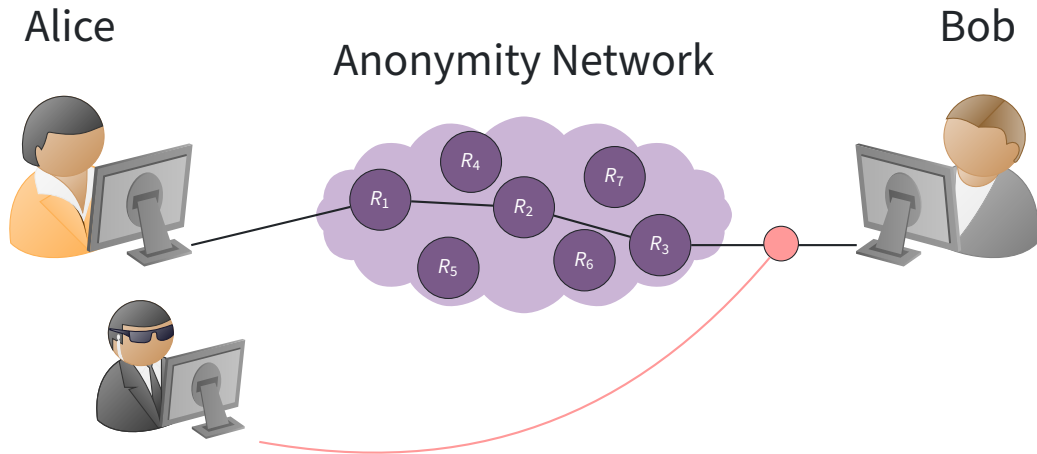
Threat Model



Threat Model



Threat Model

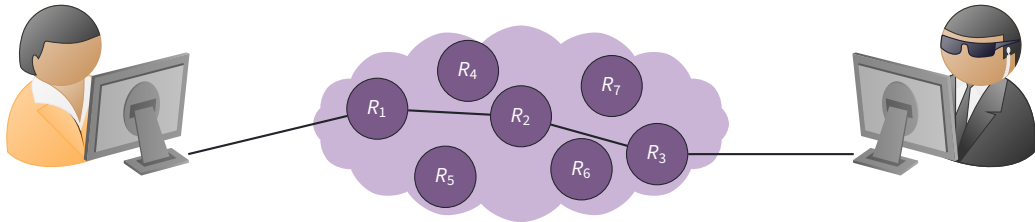


Threat Model

Alice

Anonymity Network

Bob



Anonymity isn't Encryption

Alice

Bob



...RG9uJ3QgdXNlIGJhc2U2NCBmb3IgZW5jcnlwdGlvbi4...



Gibberish!

Encryption just protects contents.

Communications Metadata



"We Kill People Based on Metadata."

—Michael Hayden, former director, NSA.

Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps - Tor Browser

Attorney General Bill Barr W × +

https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption 110%

TECH

Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps

"We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety."

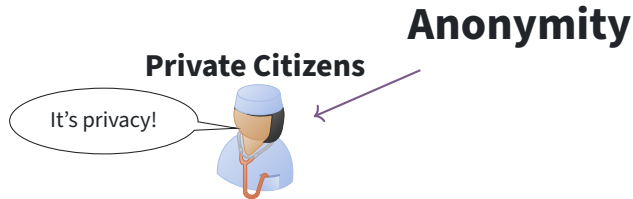
 **Ryan Mac**
BuzzFeed News Reporter

 **Joseph Bernstein**
BuzzFeed News Reporter

Last updated on October 3, 2019, at 3:28 p.m. ET
Posted on October 3, 2019, at 1:36 p.m. ET

 [Tweet](#)  [Share](#)  [Copy](#)

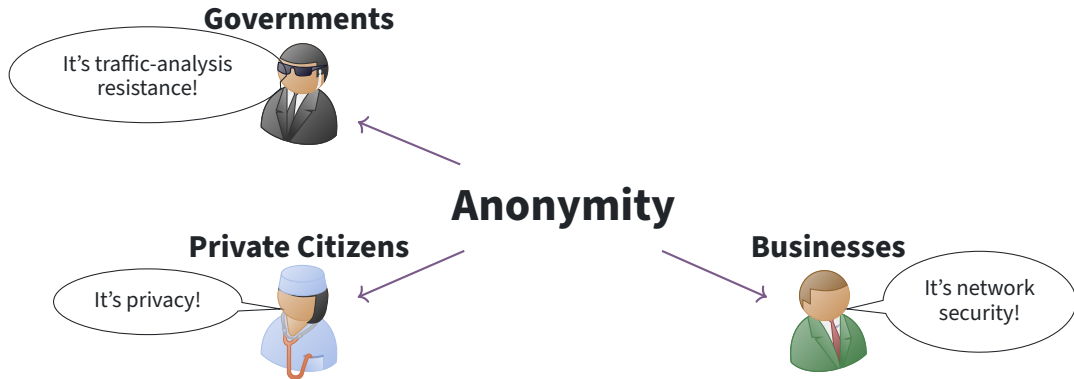
Anonymity is different for each use case



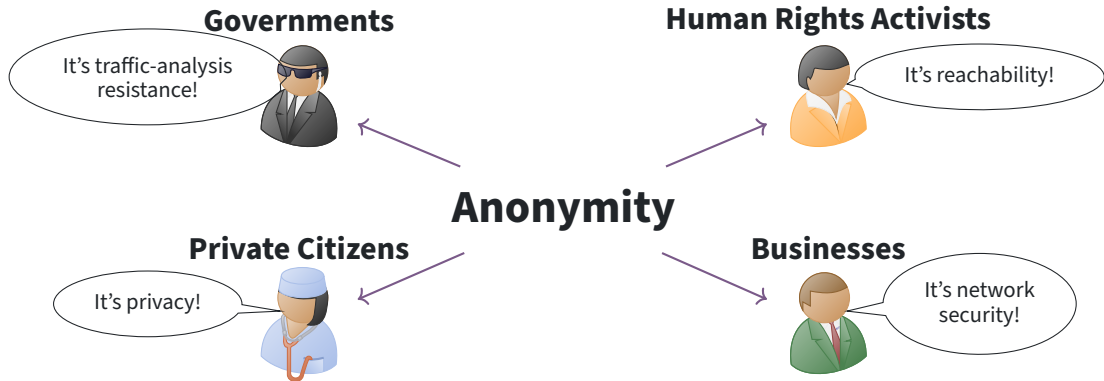
Anonymity is different for each use case



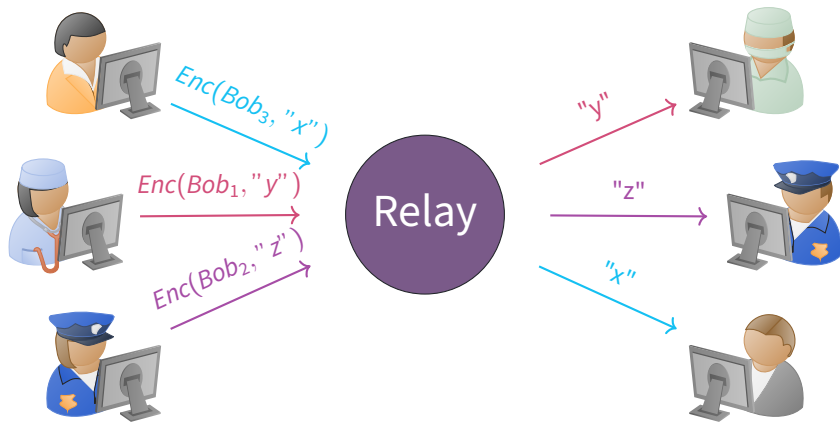
Anonymity is different for each use case



Anonymity is different for each use case

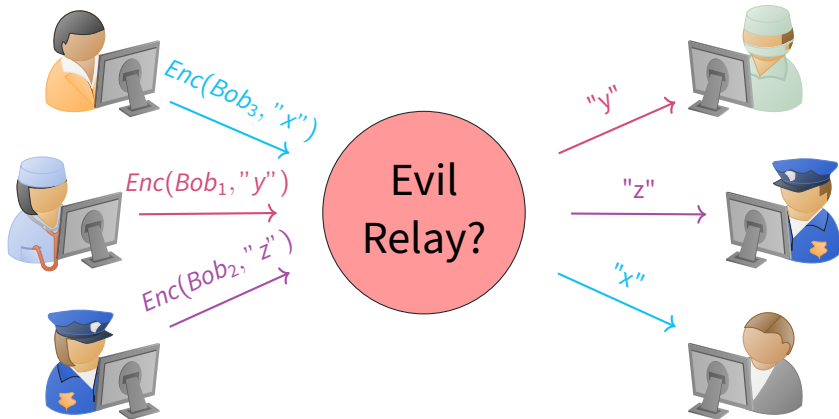


A Simple Design

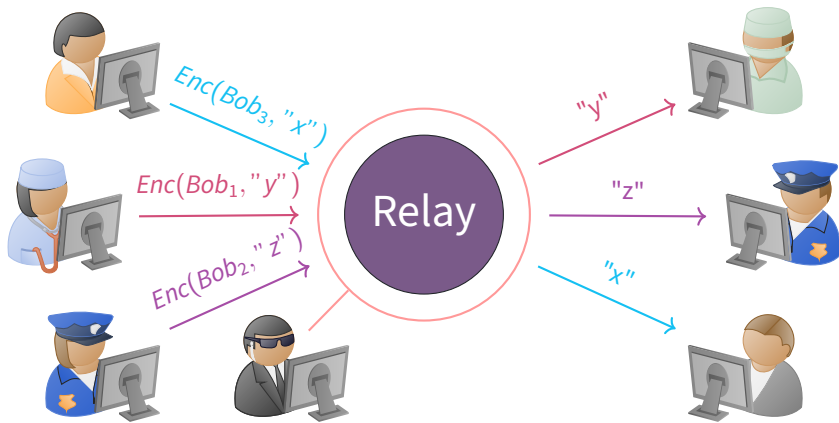


Equivalent to most commercial proxy/VPN providers.

A Simple Design

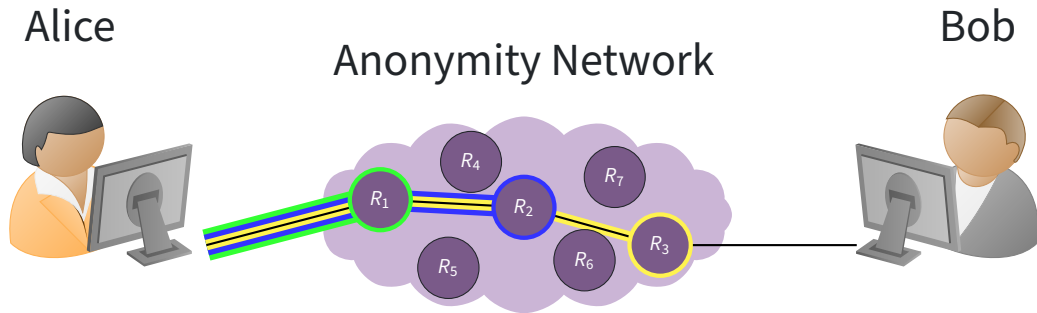


A Simple Design



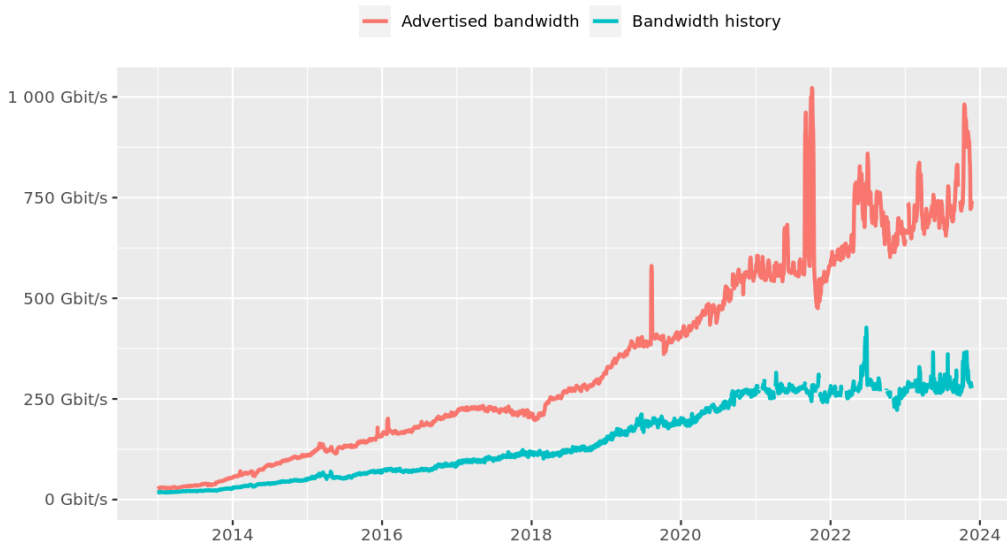
Timing analysis lets an observer match up connections.

The Tor Design



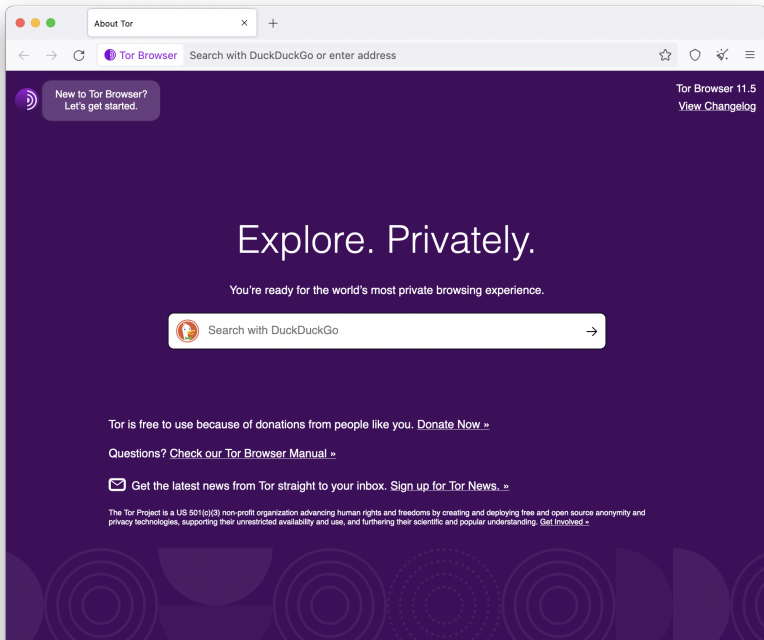
Multiple relays so no single relay can link Alice to Bob.

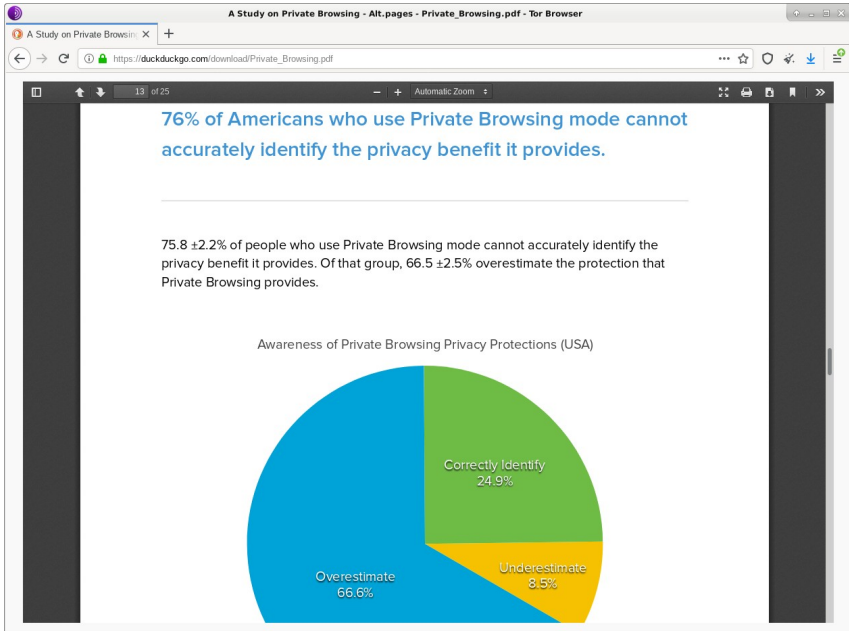
Total relay bandwidth

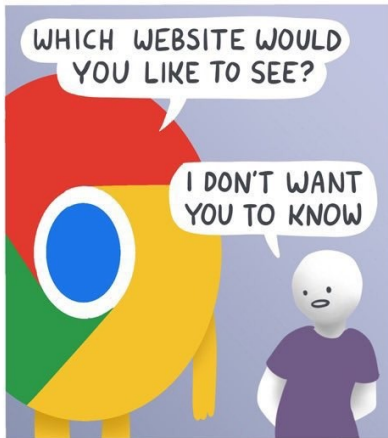


Tor's **safety** comes from **diversity**

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. Research problem: How do we measure diversity over time?
2. Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.







@SKELETON_CLAW



SKELETONCLAW.COM

Transparency for Tor is key

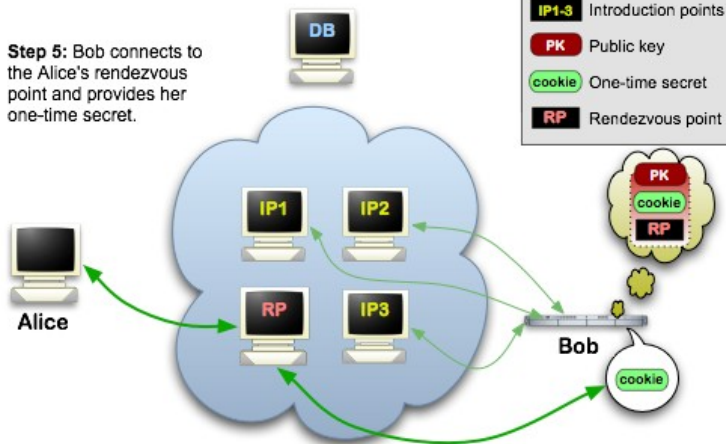
- Open source / free software
- Public design documents and specifications
- Publicly identified developers

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!

Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Onion service properties

- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor





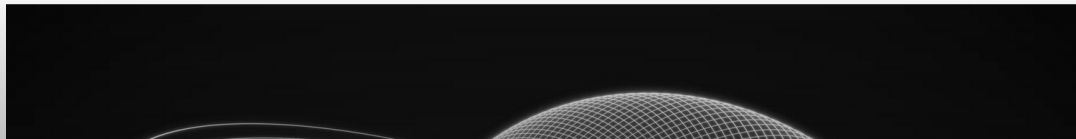
JOSEPH COX

OPINION

JUN 18, 2015 7:00 AM

The Dark Web as You Know It Is a Myth

The dark web actually has promise. In essence, it's the World Wide Web as it was originally envisioned.







1 Million People use Facebook over Tor



FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've [written previously](#) it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

BBC Blogs - Technology & Creativity Blog - Leveraging the Tor Network to circumvent blocking of BBC News content - Tor Browser

BBC Blogs - Technology & Creativity Blog

https://www.bbc.co.uk/blogs/internet/entries/936e460a-03b3-41db-be96-a6f2f27934e6

BBC

Sign in

News

Sport

Reel

Worklife

Travel

Future

More

Search

Technology + Creativity Blog

Previous

Home

Next

Leveraging the Tor Network to circumvent blocking of BBC News content

Wednesday 30 October 2019, 8:18



Abdallah al-Salmi
Strategy Analyst, BBC News

Tagged with: [BBC News](#), [BBC World Service](#), [Media Distribution](#), [Public Service](#)

COMMENTS

The BBC World Service's news content [became available on the Tor Network last week](#) in a move that attracted wide media attention.

The decision to go ahead with setting this service up came at a time when BBC News is either blocked or restricted in several parts of the world.

For example, in Egypt, Iran and China, our audiences are finding it either impossible or difficult to access our content without the use of a circumvention tool, such as a VPN.

The Tor Network is an overlay network on the internet, which provides increased security and is resistant to blocking.

About this Blog



Staff from the BBC's online and technology teams talk about BBC Online, BBC iPlayer, BBC Red Button and the BBC's digital services. The blog is reactively moderated. Your host is Jonathan Murphy.

Follow [Technology & Creativity Blog](#) on Twitter

[Blog home](#)
[Explore all BBC blogs](#)

Blog Updates

Stay updated with the latest posts from the blog

31

Contact Sales: +1 (888) 274-3482



The Cloudflare Blog

Keep up to date with Cloudflare's latest news. Subscribe to the Blog.

Email Address

Subscribe

Product News

Speed & Reliability

Security

Serverless

Cloudflare Network

Developers

Deep Dive

Life @Cloudflare



Introducing the Cloudflare Onion Service

[Tweet](#)

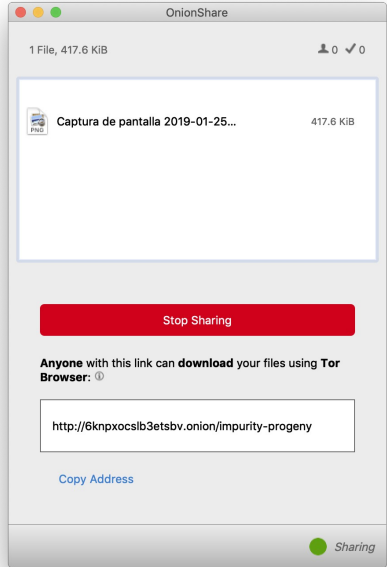
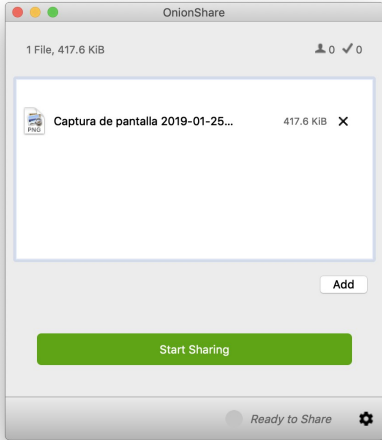


Mahrud Sayrafi

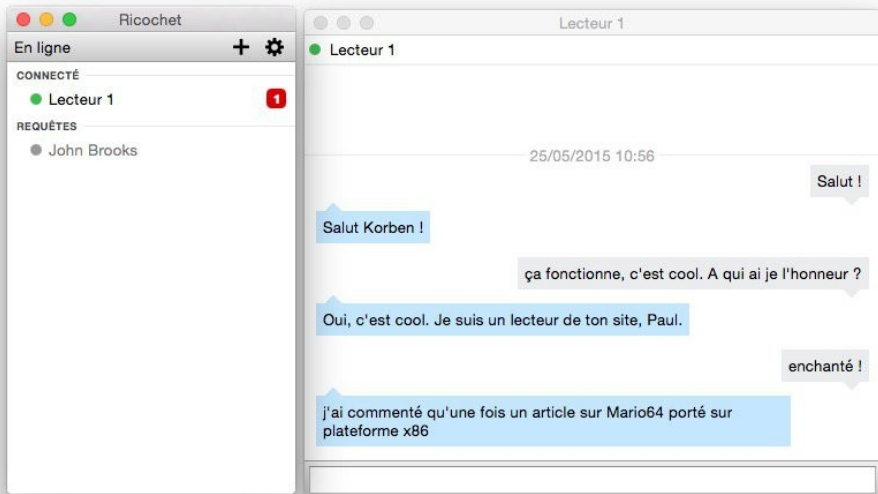
September 20, 2018 12:00PM



OnionShare



Ricochet

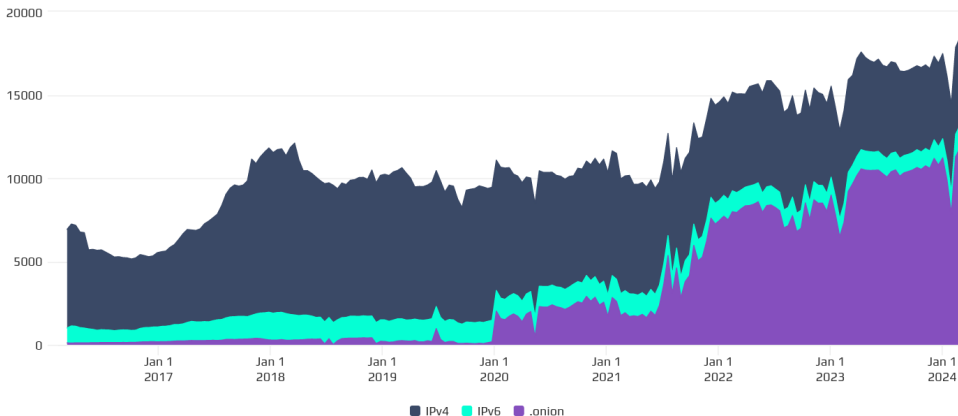


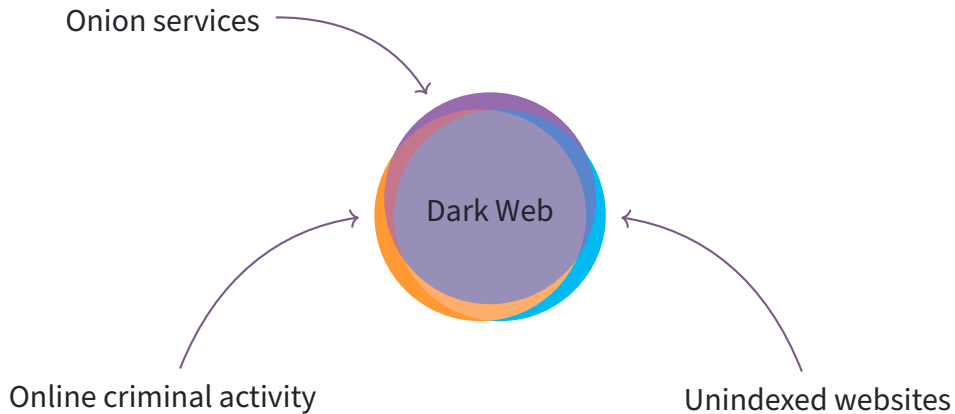
NODES

Chart shows the number of reachable Bitcoin nodes during the last 8 years. Series can be enabled or disabled from the legend to view the chart for specific networks.

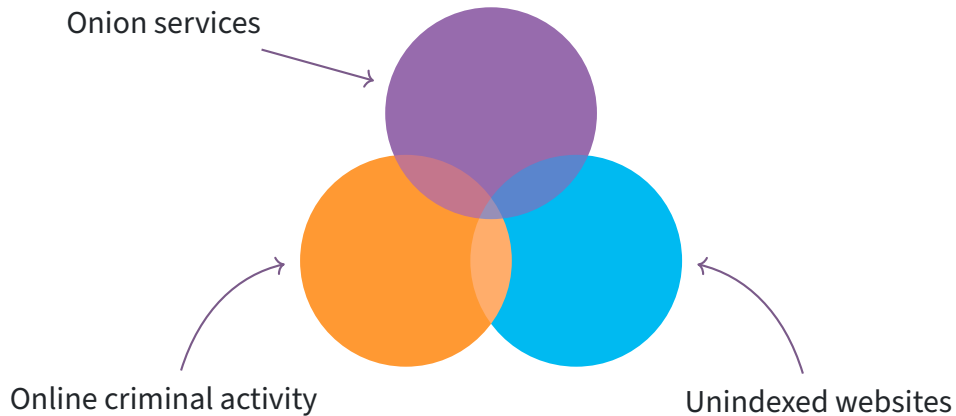
24h 90d 1y 8y

Lo 5152 Hi 18424 Avg 11120 Last 18424 nodes

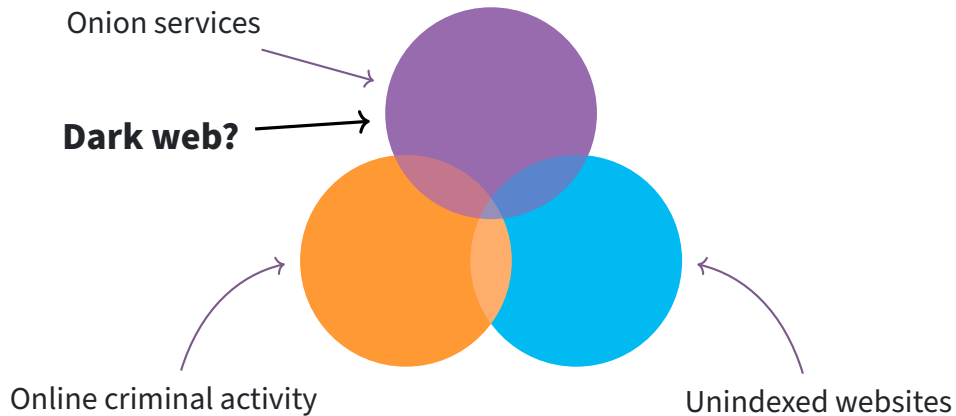




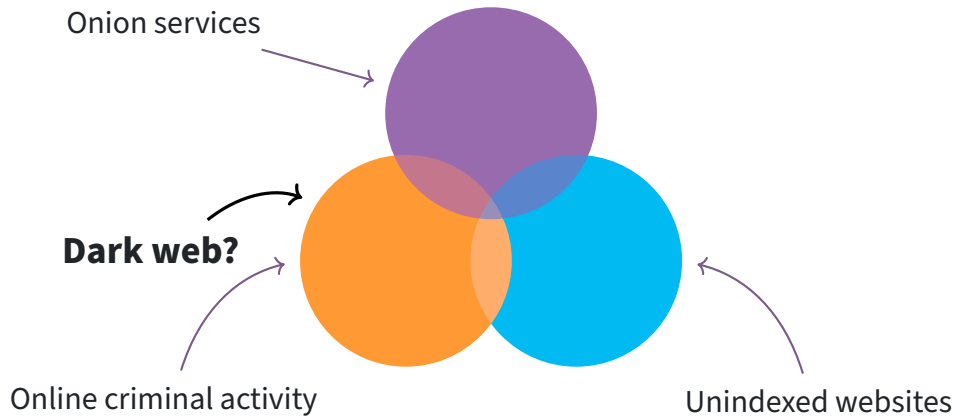
The "Dark Web" as popularly depicted



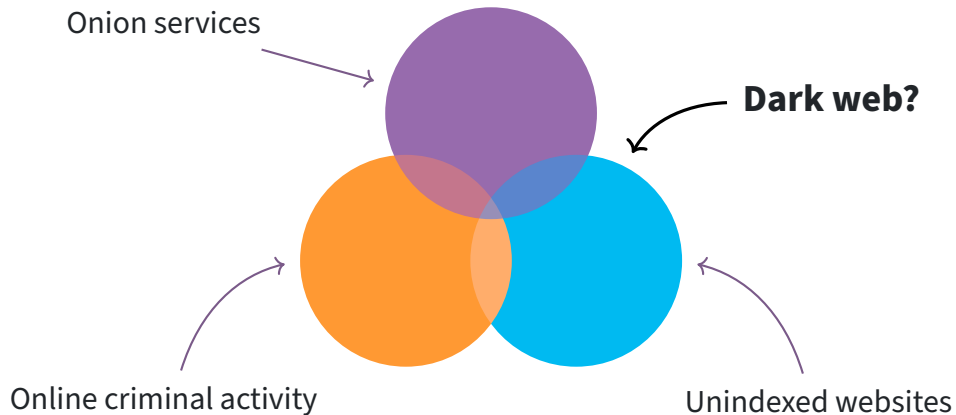
Closer to reality



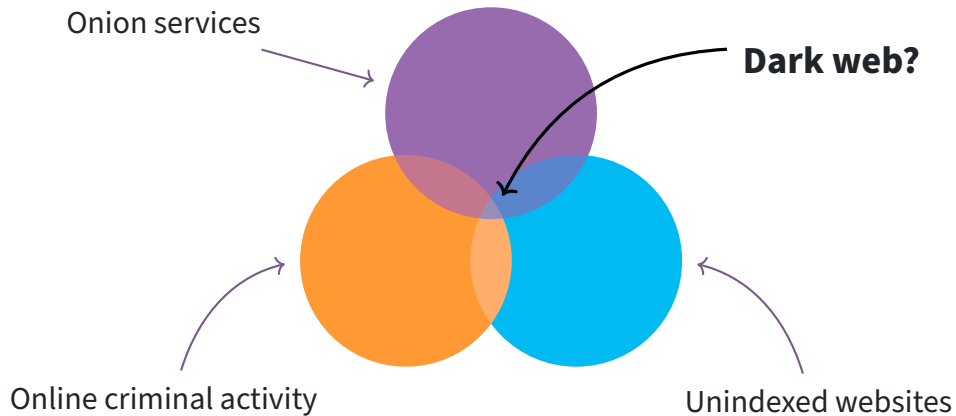
Closer to reality



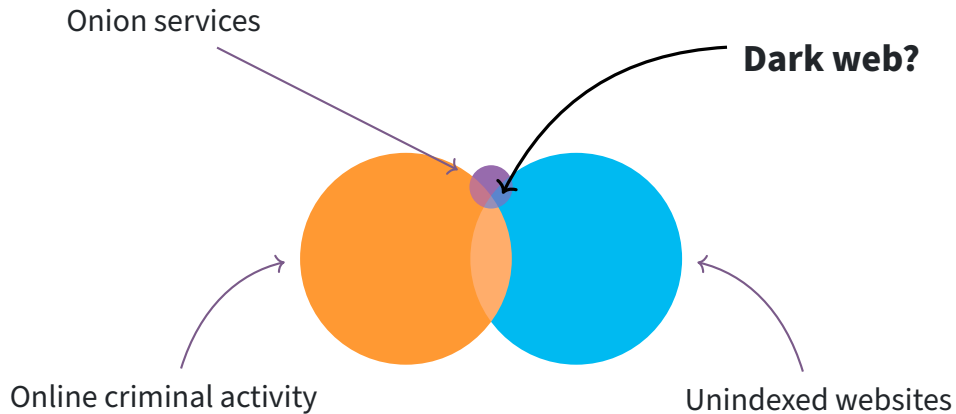
Closer to reality



Closer to reality



Closer to reality



Scale also matters



Onion Services: Step 1

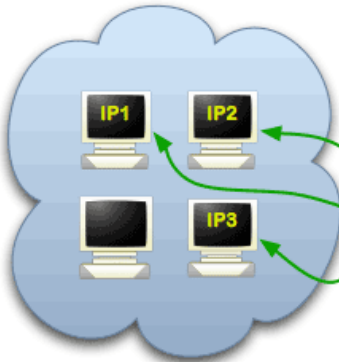
Step 1: Bob picks some introduction points and builds circuits to them.



Alice



DB



Bob

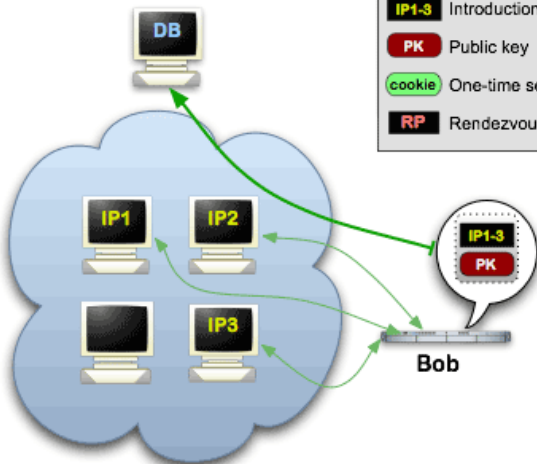


Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.



Alice

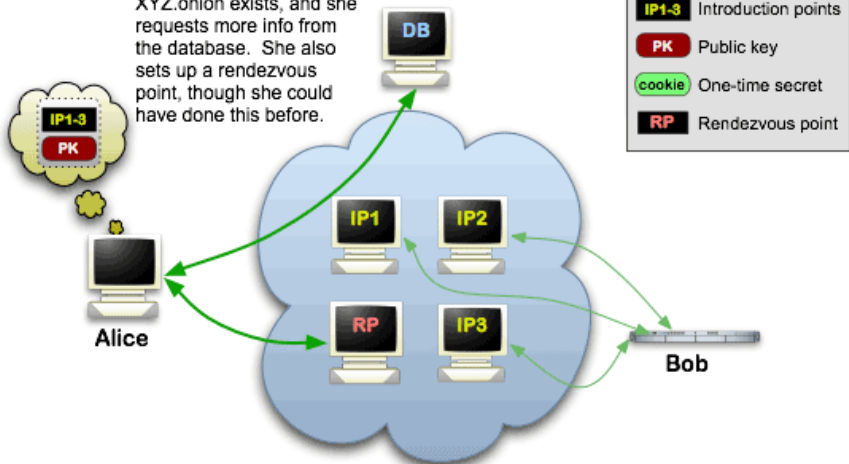


	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	Rendezvous point



Onion Services: Step 3

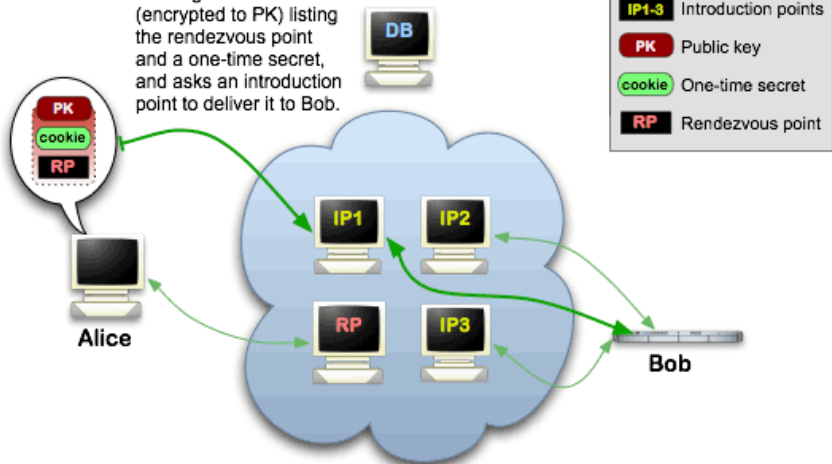
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.





Onion Services: Step 4

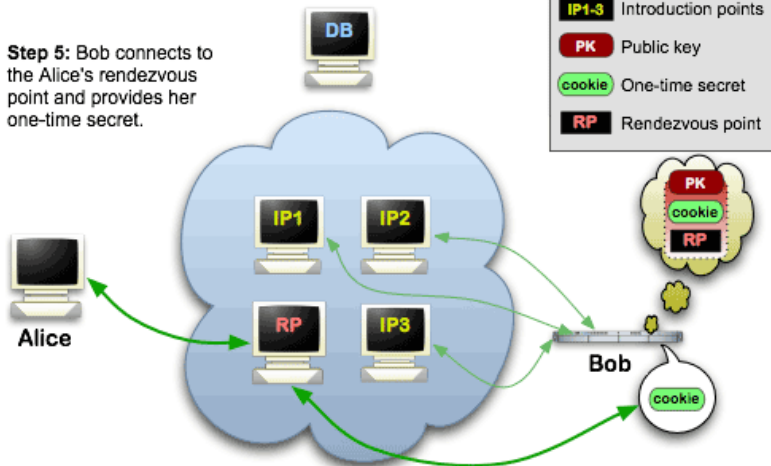
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.





Onion Services: Step 5

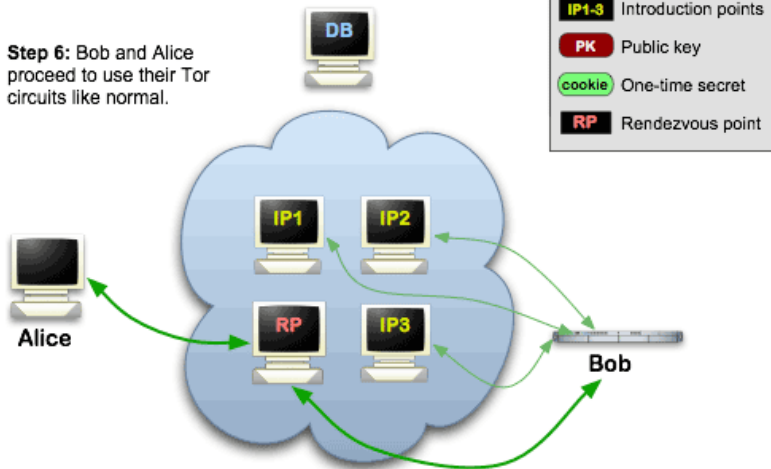
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.





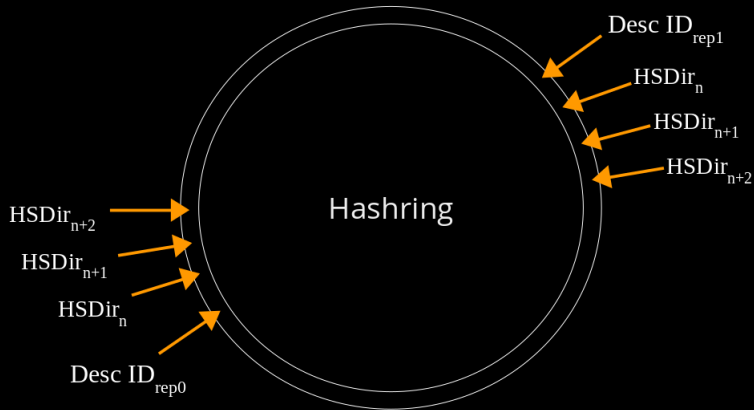
Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



HS Directory

Desc ID = $H(\text{onion-address} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$



Flaw: HSDir relays were too predictable

The six daily HSDirs for a given onion address were predictable into the future.

So a bad guy could run six relays with just the right keys to target a specific future day... to censor or to measure popularity.

A few people—we don't know who—were doing this attack in practice.

Fix: Global shared random value

Make the HSDir mapping include a communal random value that everybody agrees about but that nobody can predict.

The directory authorities pick this value each day as part of their consensus voting process.

Flaw: HSDirs got to learn onion addresses

The onion service descriptor (which gets uploaded to the HSDir) included the public key for the service (so everybody can check the signature).

So you could run relays and discover otherwise-unpublished onion addresses.

“Threat intelligence” companies were trying to do just that.

Fix: New crypto hides the address

The new ed25519 cryptosystem has a cool feature where you can sign the onion descriptor with a subkey.

So everybody can check the signature but nobody can learn the main key from the subkey or signature.

Should finally kill the arms race with jerks running relays to gather onions.



SMART INDIA
HACKATHON
2023



SMART INDIA
HACKATHON
2023

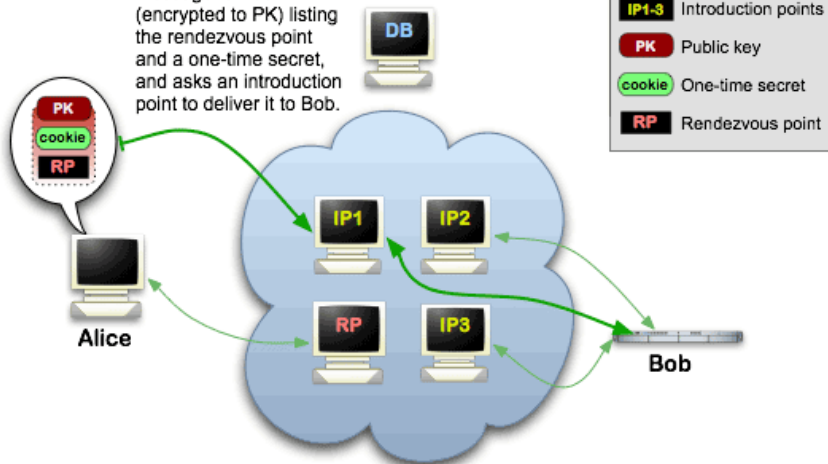
PROBLEM STATEMENT DETAILS

Problem Statement ID	1455
Problem Statement Title	Efficient enumeration of URLs of active hidden servers over anonymous channel (TOR)
Description	The Onion Routing (TOR) is an overlay anonymous network over internet, which not only anonymizes clients accessing the TOR network or internet but also facilitate hosting of servers anonymously. These servers have been reported to be hosting various hidden services involved in malicious activities. The goal of this problem statement is to develop Proof of Concept (PoC) to enumerate URLs (.onion) of active hidden servers hosted over TOR. Teams are supposed to examine the cryptographic security controls and survey existing vulnerabilities in underlying security architecture of TOR network to develop PoC for efficient enumeration of URLs of active hidden services hosted over TOR.
Organization	National Technical Research Organisation,(NTRO)
Category	Software
Domain Bucket	Blockchain & Cybersecurity
Youtube Link	
Dataset Link	NA



Onion Services: Step 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

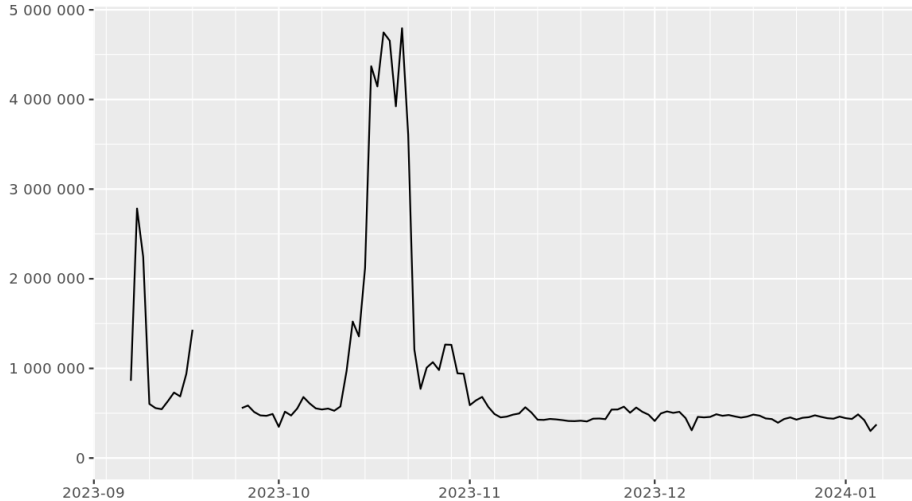


You can send many many introductions

For example, if you want to deny service to a target onion service, spin up millions of Tor clients and have each of them try to visit it.

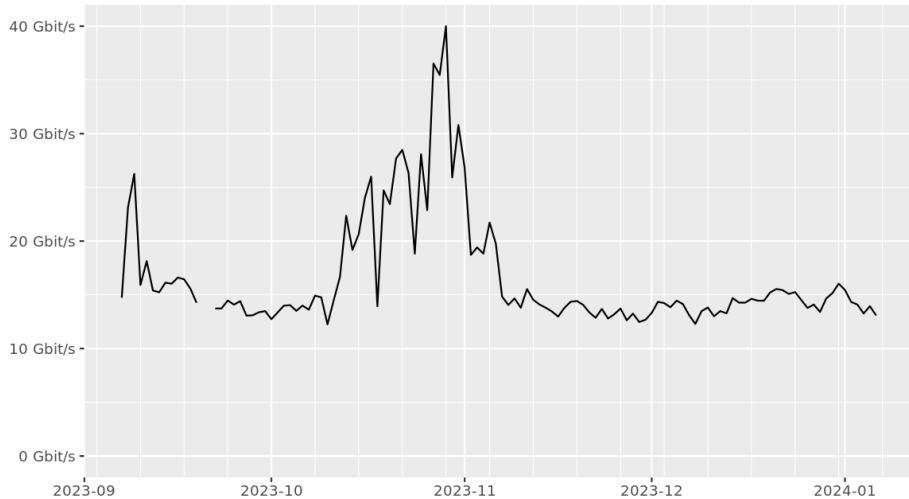
It's an anonymity system (!) so the service can't tell which intro cells to drop and which to answer.

Directly connecting users from the United States



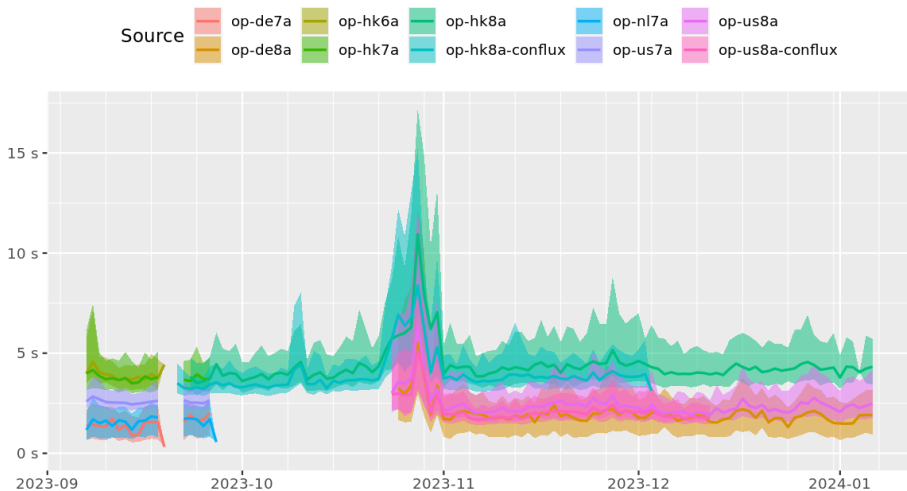
The Tor Project - <https://metrics.torproject.org/>

Onion-service traffic v3



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

Time to complete 1 MiB request to public server



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

Fix: integrate PoW into the intro cell

Onion services, when under attack, advertise a suggested effort level in their onion descriptor.

Clients see the effort level and bid for attention (“blind auction” in economics terms).

The service side sorts the incoming intro cells, then answers best effort.

PoW in the intro cell

Service should follow a feedback loop: raise effort if it can't keep up, lower effort if it is keeping up.

The PoW we've picked aims to not be FPGA/ASIC friendly.

Still some messy design questions, e.g. at what rate (how many) should we try to answer?

But what about...

Doesn't this favor desktops over mobiles?

I thought PoW/bitcoin destroyed the climate?

Why do you want to help *those* onion services?

HEAD ▾

torspec / proposals / 327-pow-over-intro.txt

Find file

Blame

History

Permalink

 **327-pow-over-intro.txt**  57.58 KIB

Blame

Edit ▾

Replace

Delete



```
1  '''
2  Filename: 327-pow-over-intro.txt
3  Title: A First Take at PoW Over Introduction Circuits
4  Author: George Kadianakis, Mike Perry, David Goulet, tevador
5  Created: 2 April 2020
6  Status: Closed
7
8  0. Abstract
9
10 This proposal aims to thwart introduction flooding DoS attacks by introducing
11 a dynamic Proof-Of-Work protocol that occurs over introduction circuits.
12
13 1. Motivation
14
15 So far our attempts at limiting the impact of introduction flooding DoS
16 attacks on onion services has been focused on horizontal scaling with
17 Onionbalance, optimizing the CPU usage of Tor and applying rate limiting.
18 While these measures move the goalpost forward, a core problem with onion
19 service DoS is that building redundant circuits is a costly procedure both
```

Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis

Calls to action

Understand the risks of centralized architectures

Fight the slippery slope that is internet censorship

Participate in privacy / censorship research, e.g.

<https://petsymposium.org/>

<https://foci.community/>

Volunteer as a relay, a bridge, or a snowflake!