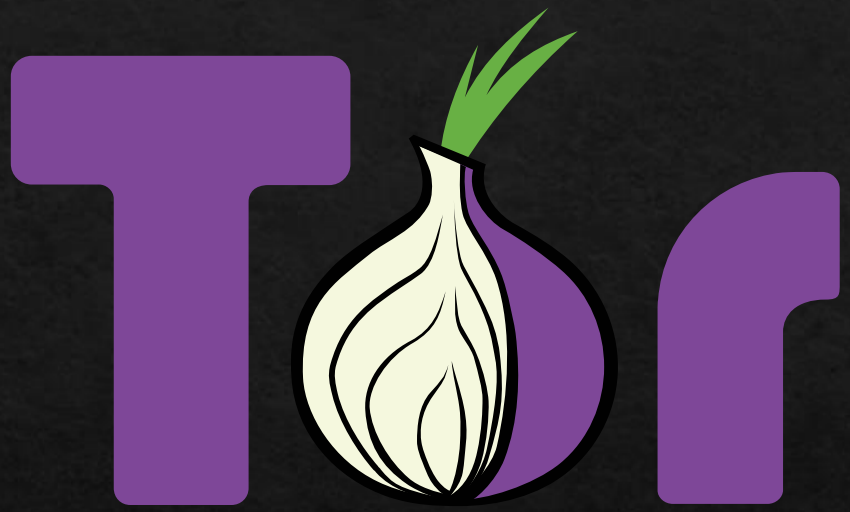


Anonymous Connections
and Onion Routing

A Seminar by Chris Scott, Bofeng Li, and Eamon O'Brien

Onion Routing

Why is it needed?

Network Anonymity

Original Goals

- Classic TCP/IP requests secured with SSL
- Sent directly to receiver and back
- Both receiver significant information about each other

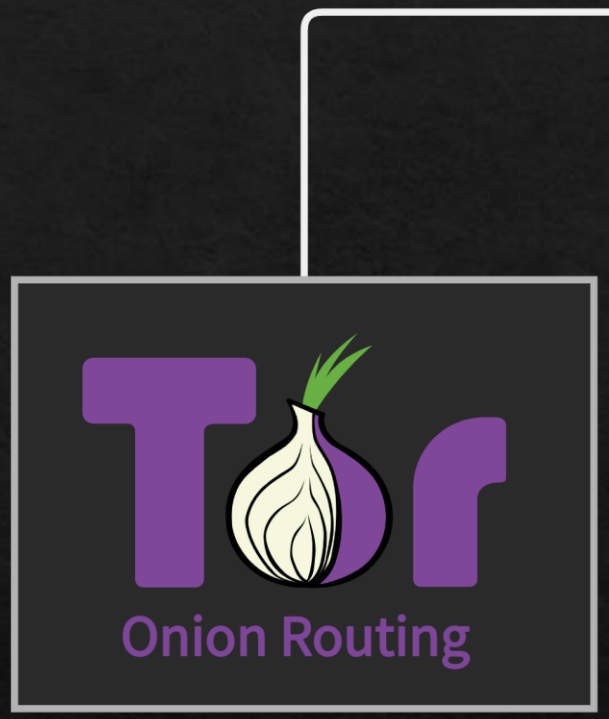
- Onion Routing forwards through network
- Also stripped of all user data
- Fully anonymises sender and receiver

Images: (Pixabay.com)

Onion Routing

OSI Model Overview

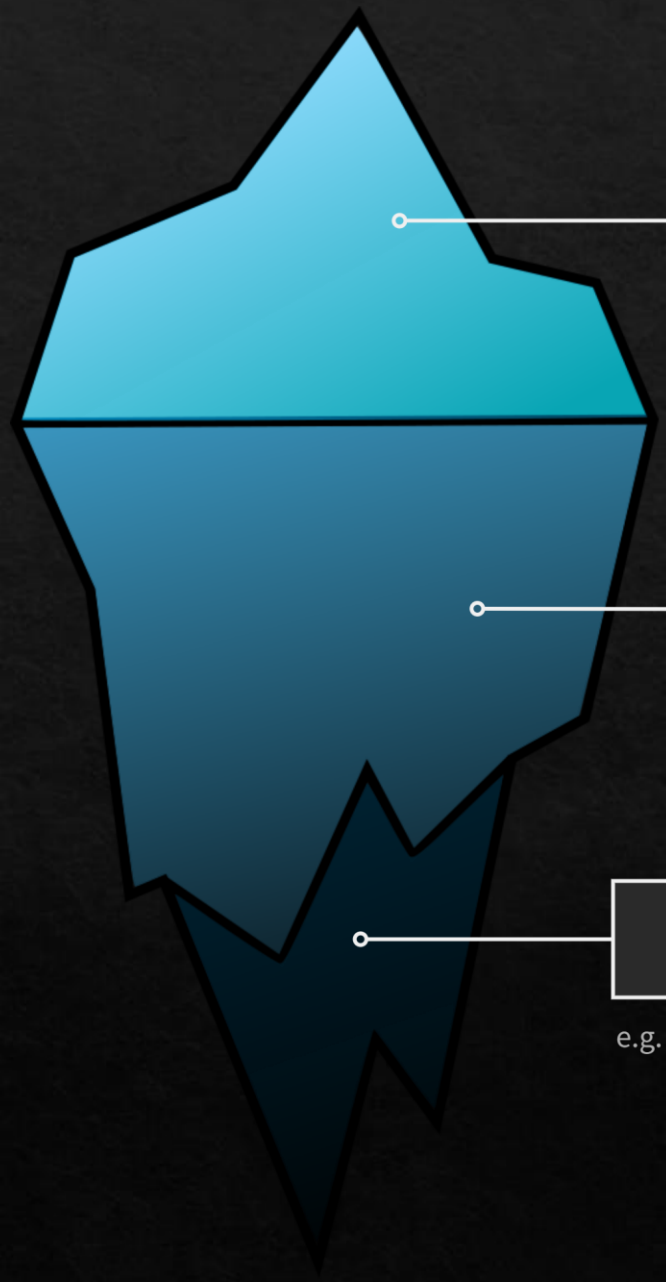
TOR operates on the **Application Layer** and uses **TCP/IP** (Transport Layer) for transport.



7	Application Layer
	HTTP, FTP, IRC, SSH, DNS, etc.
6	Presentation Layer
	SSL, SSH, IMAP, FTP, JPEG, PNG, etc.
5	Session Layer
	API's, Sockets, WinSock, etc.
4	Transport Layer
	TCP, UDP, etc.
3	Network Layer
	IP, ICMP, IPsec, IGMP, etc.
2	Data Link Layer
	Ethernet, PPP, Switches, Bridges, etc.
1	Physical Layer
	Coax, Fibre, Twisted Pair, Wireless, etc.

Onion Routing

Layers of the Web



Surface Web

Information that **is** indexed by Search Engines.

e.g. YouTube, Wikipedia, Google etc.

Deep Web

Information that **is not** indexed by Search Engines.

e.g. Academic Records, Netflix, Pay-Walled Content etc.

Dark Web

Information that is only accessible using **specific hardware/software.**

e.g. Overlay Networks (TOR, IP2 etc.)

Onion Routing

Usage

2.6 Billion
Google Chrome Users

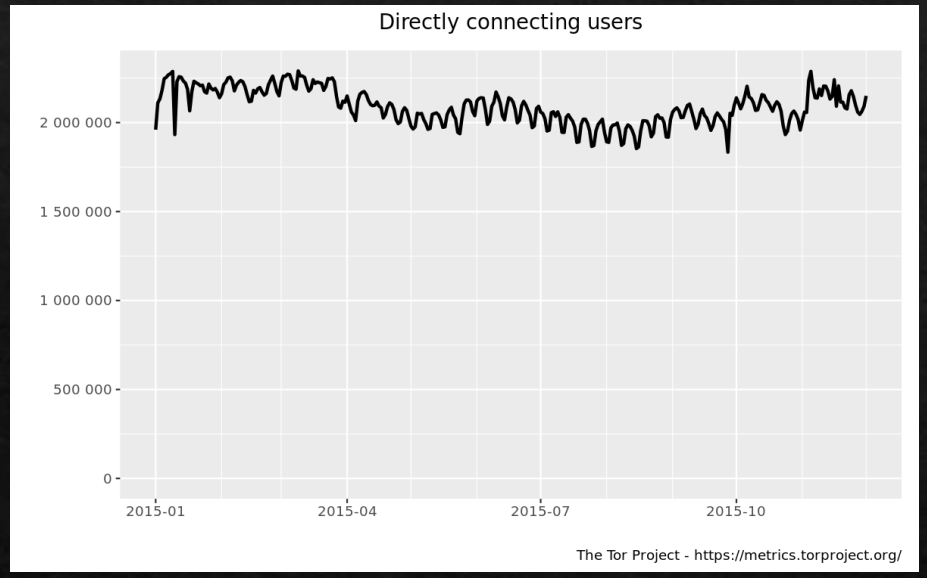
2 Million
TOR Users

60,000
Hidden Services Users

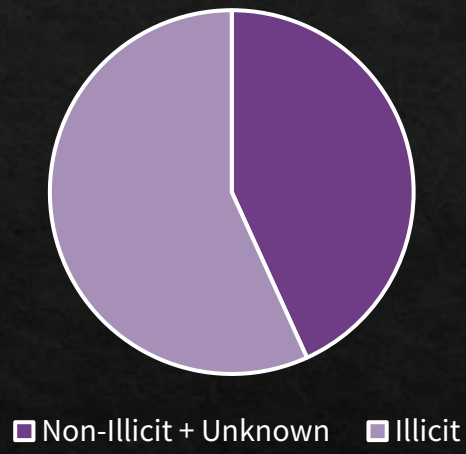
As of 2020.
Sources: (Statista, World Wide Browser Usage), (Tor User Metrics, The TOR Project)

Onion Routing

Key Uses



Web-based Onion Services



As of 2016.
Source: (Moore et al., 2016)

User Anonymity

The Tor Project measured upwards of 2 million daily users in 2015, 96.6% of which connected to publicly available web.

As of 2015.
Sources: (Tor User Metrics; Some Statistics About Onions, The Tor Project)

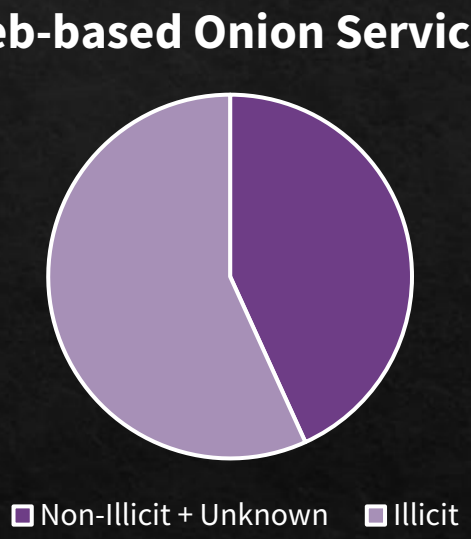
Criminal Activity

Of the users who did not, it is estimated that the .onion websites available were approximately 43.2% of the total.

However, the remaining 56.8% were suspected criminal, extremist, illicit, violent, and/or other types of dangerous activities.

Criminal Operations

The Darker Side of Tor



Category	Percentage
Violence	0.60%
Arms	1.50%
Illicit Social	2.40%
Hacking	3.50%
Illicit Links	4.30%
Illicit Pornography	4.50%
Extremism	5.10%
Illicit Other	7.30%
Illicit Finance	12.00%
Illicit Drugs	15.50%
Total Illicit	56.80%

Many criminal efforts make use of the anonymous side of the Tor network, the ratio is strikingly larger than any that common browsers can access.

The Illicit services that operate favour drugs and finance, however there are other services that operate as well making up a total of 56.8% of the onion sites.

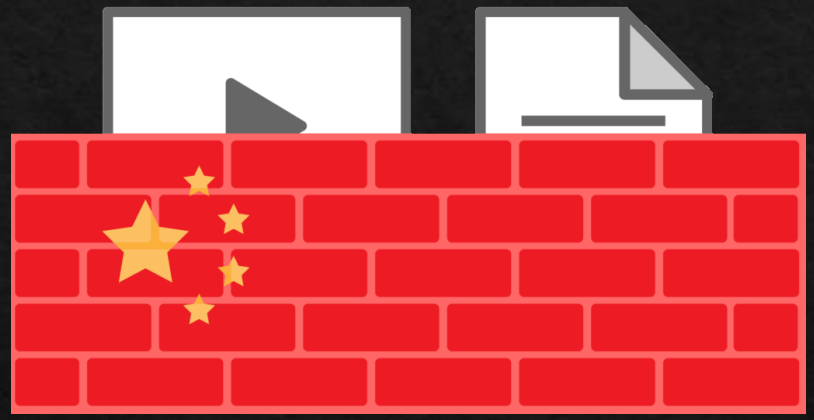
Sources: (The Tor Project, 2015), (Moore & Rid, 2016)

Freedom of Information

Tor's Role in The World

Multiple well-known domains operate proxies with onion extensions, including:

- BBC & NY Times
- The Pirate Bay
- Facebook
- And of course, the Tor Project itself



Some countries including China prefer to limit internet access within, but Tor allows greater access to these people

- Inaccessible common domains
- Censored media
- Freedom of Speech & Press

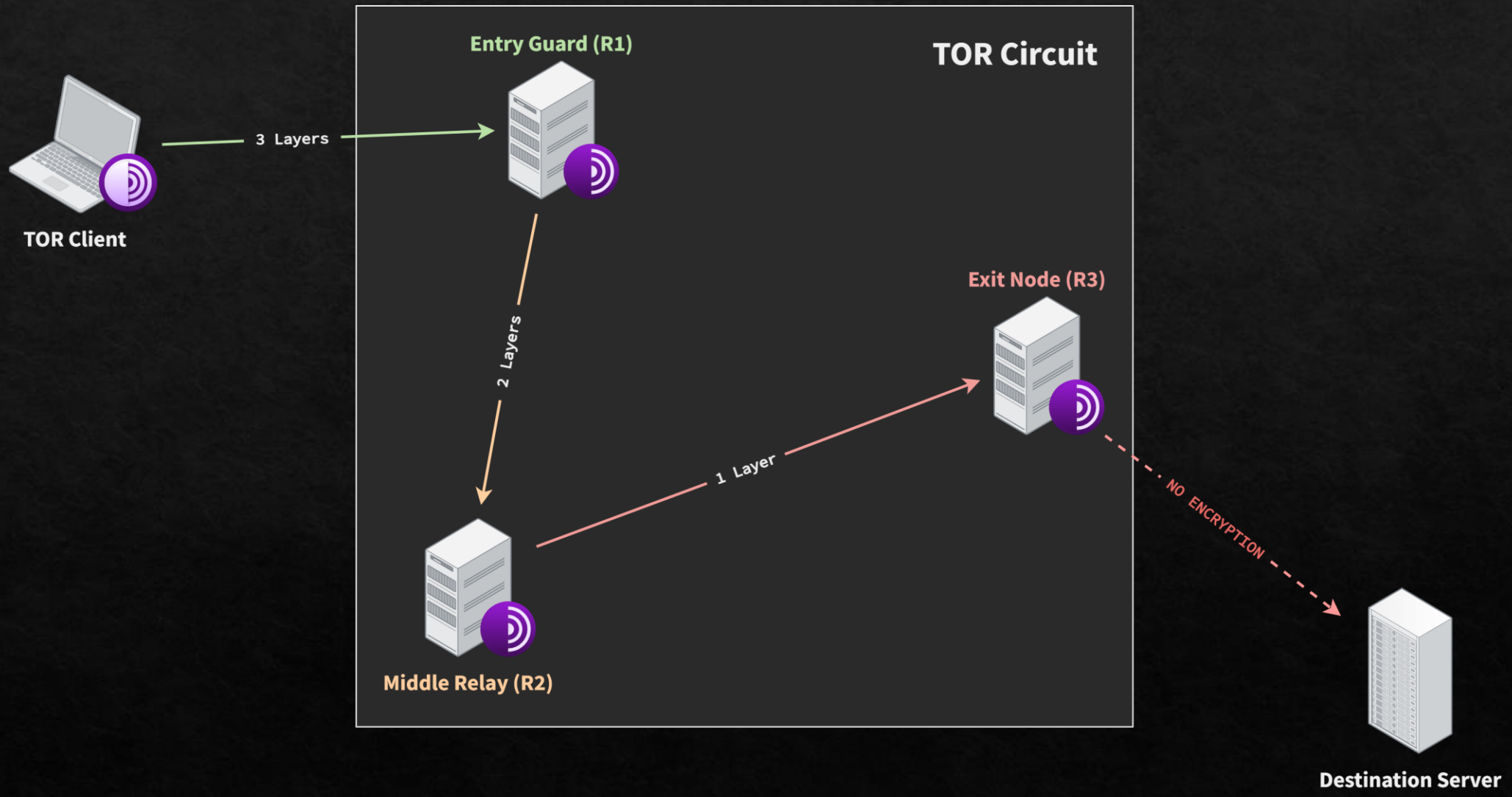
Images: (BBC, The Tor Project, The Pirate Bay), (University of Sussex)

Onion Routing

How does it work?

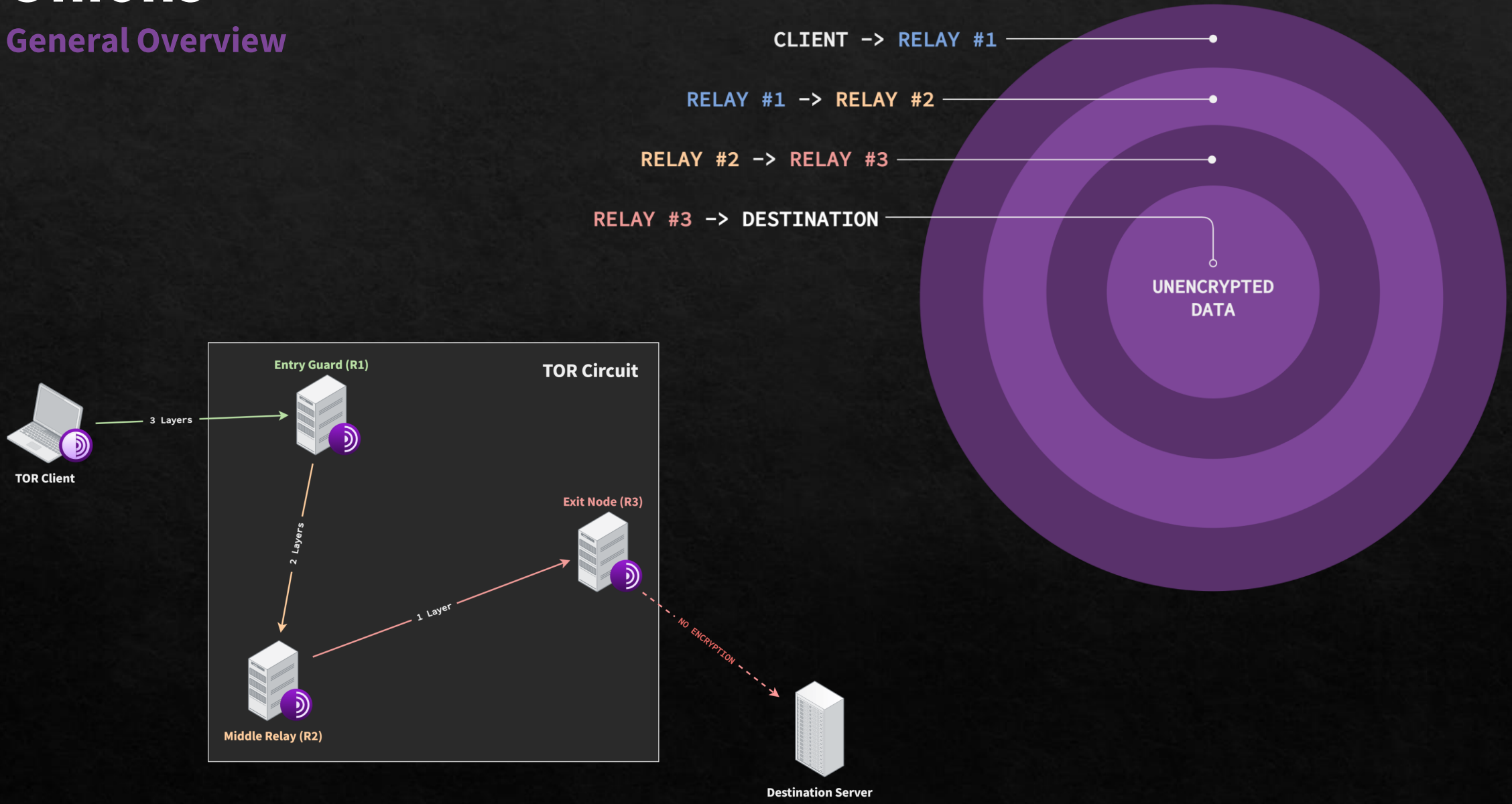
The TOR Network

General Overview



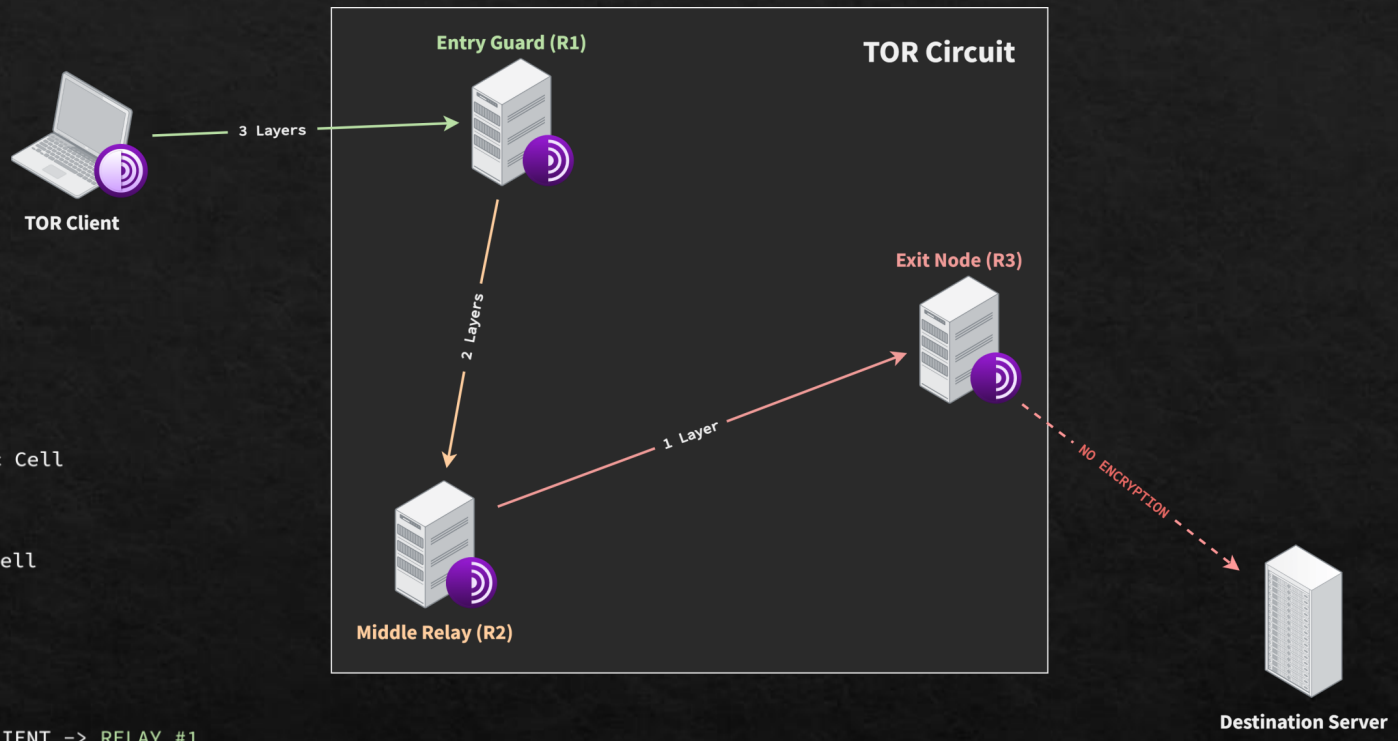
Onions

General Overview



Onions

Technical Overview



2	1	509
CircID	CMD	DATA

Generic Cell

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA

Relay Cell

C1	R1	StreamID	Digest	Len	CMD
C2	R2	StreamID	Digest	Len	CMD
C3	R3	StreamID	Digest	Len	CMD
C4					CMD
DATA					

C1: CLIENT -> RELAY #1

C2: RELAY #1 -> RELAY #2

C3: RELAY #2 -> RELAY #3

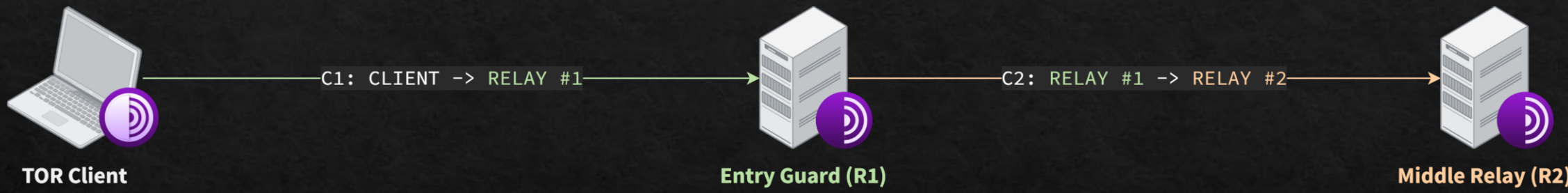
C4: RELAY #3 -> SERVER

"HTTP GET ..."

TOTAL: 512 Bytes

Onions

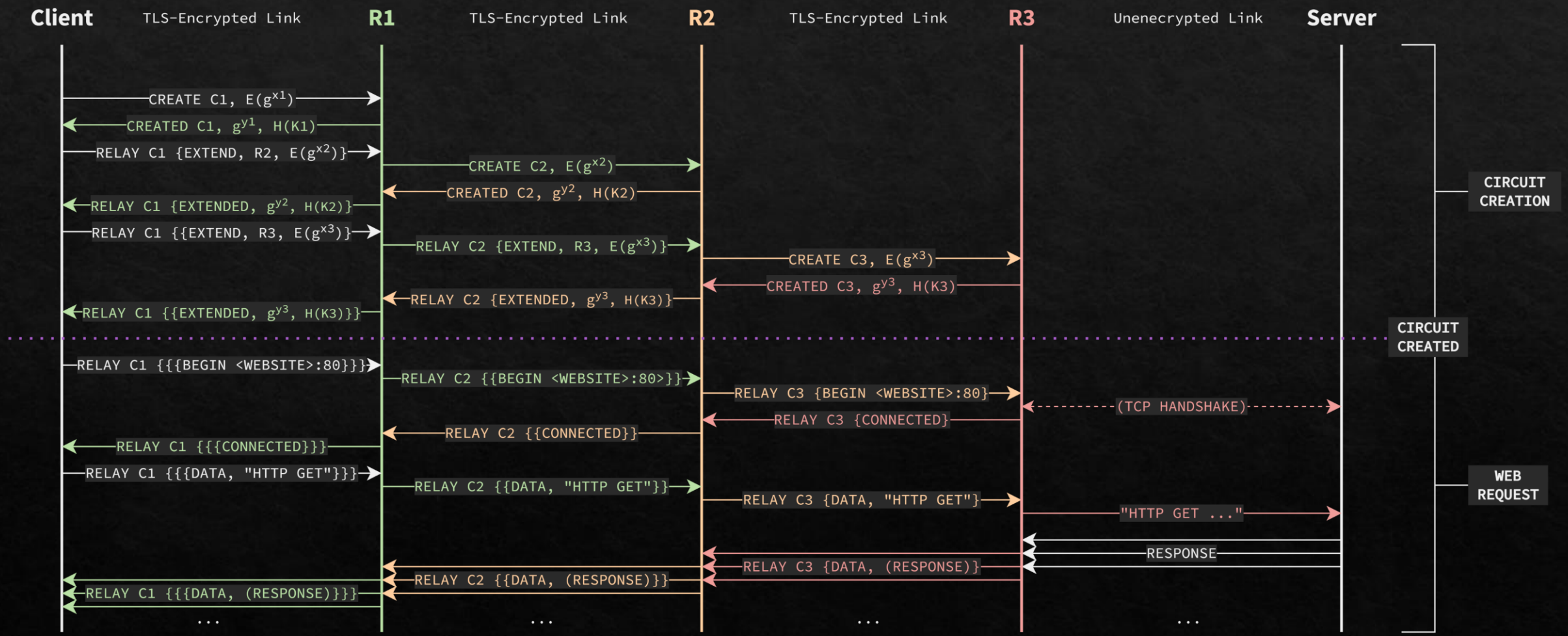
Technical Overview



TOR Communication

Technical Overview

LEGEND:
E(*) - RSA Encryption
{*} - AES Encryption
C# - A CircID



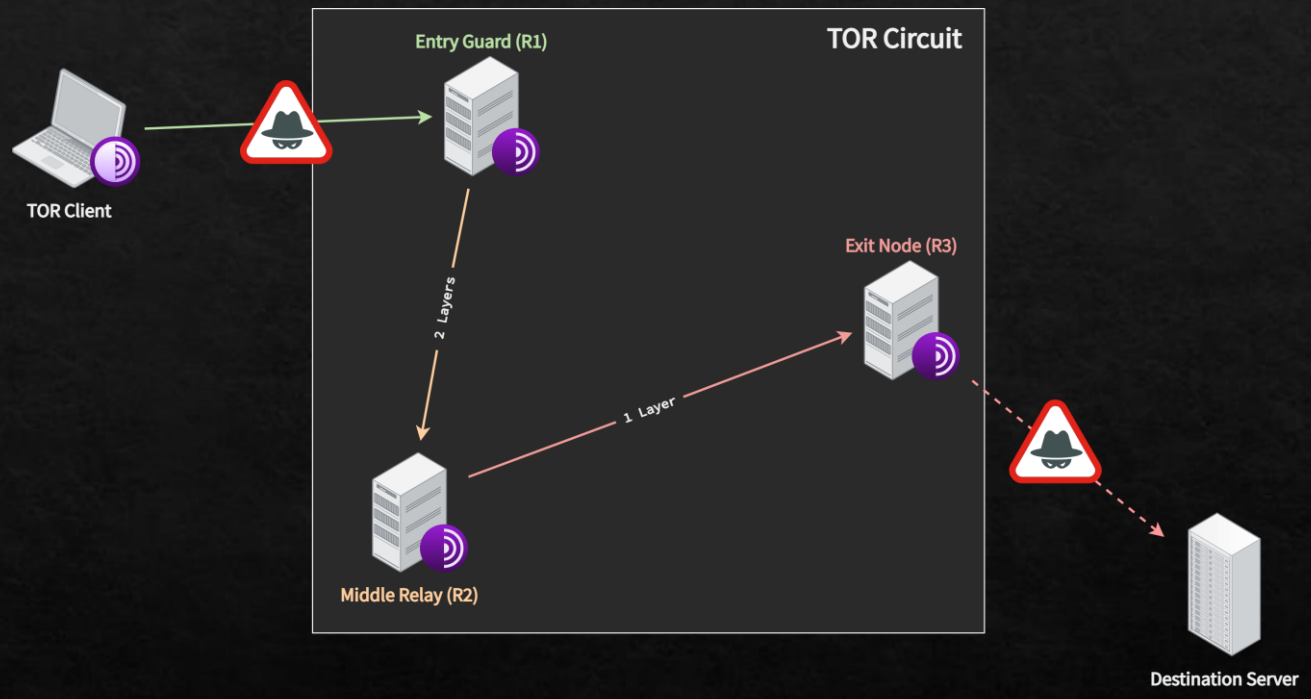
Hidden Services

Rationale

Malicious Actors who have access to both ends of the TOR network can de-anonymise users relatively easily.

How can we combat this?

Can we host the destination server **inside** the TOR network?

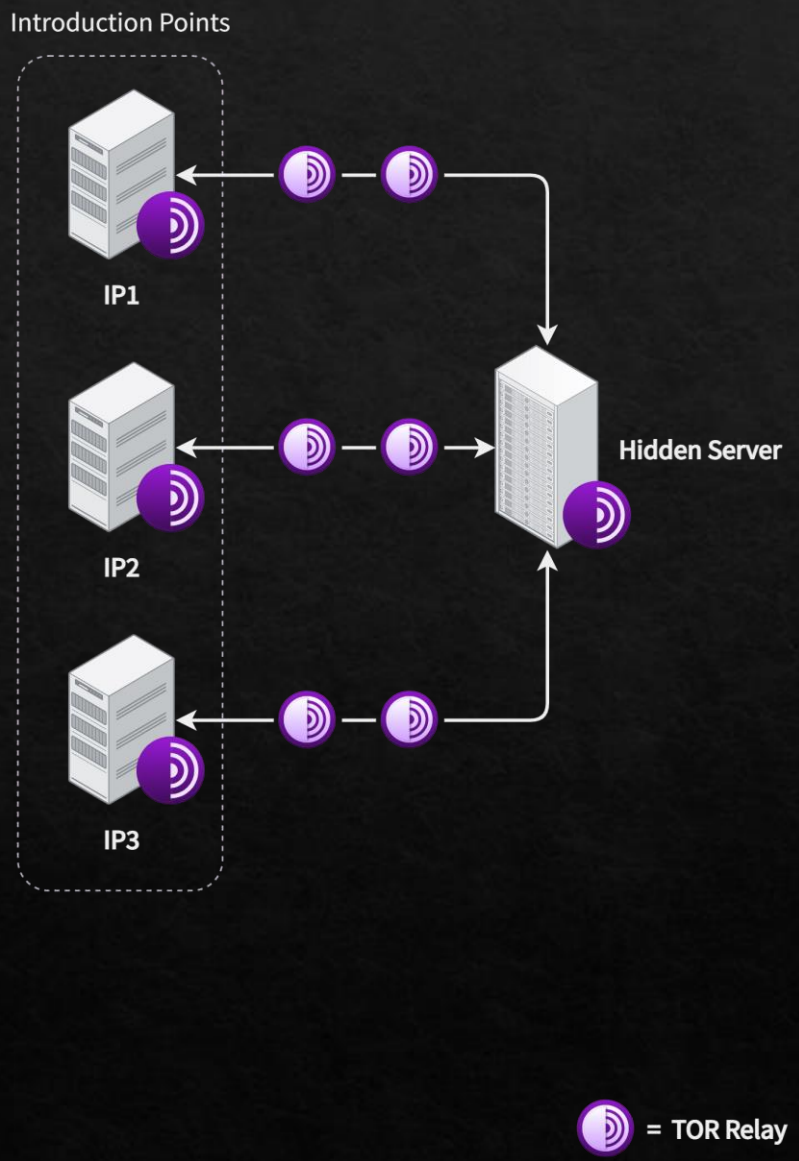


Hidden Services

General Overview

Yes, we can! By using **Hidden Services**.

A **Hidden Server** hides behind three **Introduction Points** (Relays chosen by the Hidden Server) and lives **inside** the TOR network.

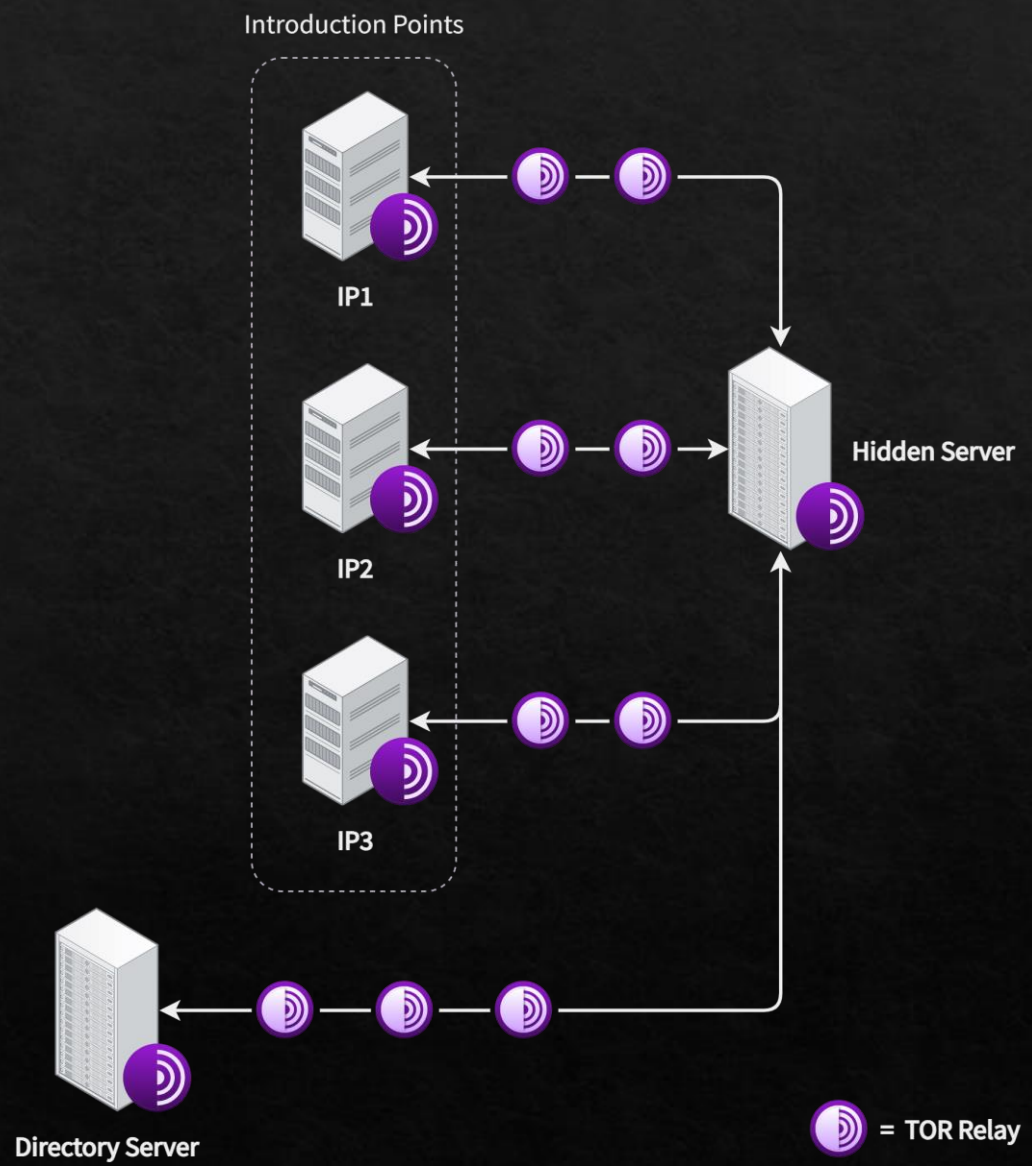


Hidden Services

General Overview

Hidden Server sends a Directory Server it's **Descriptor**.

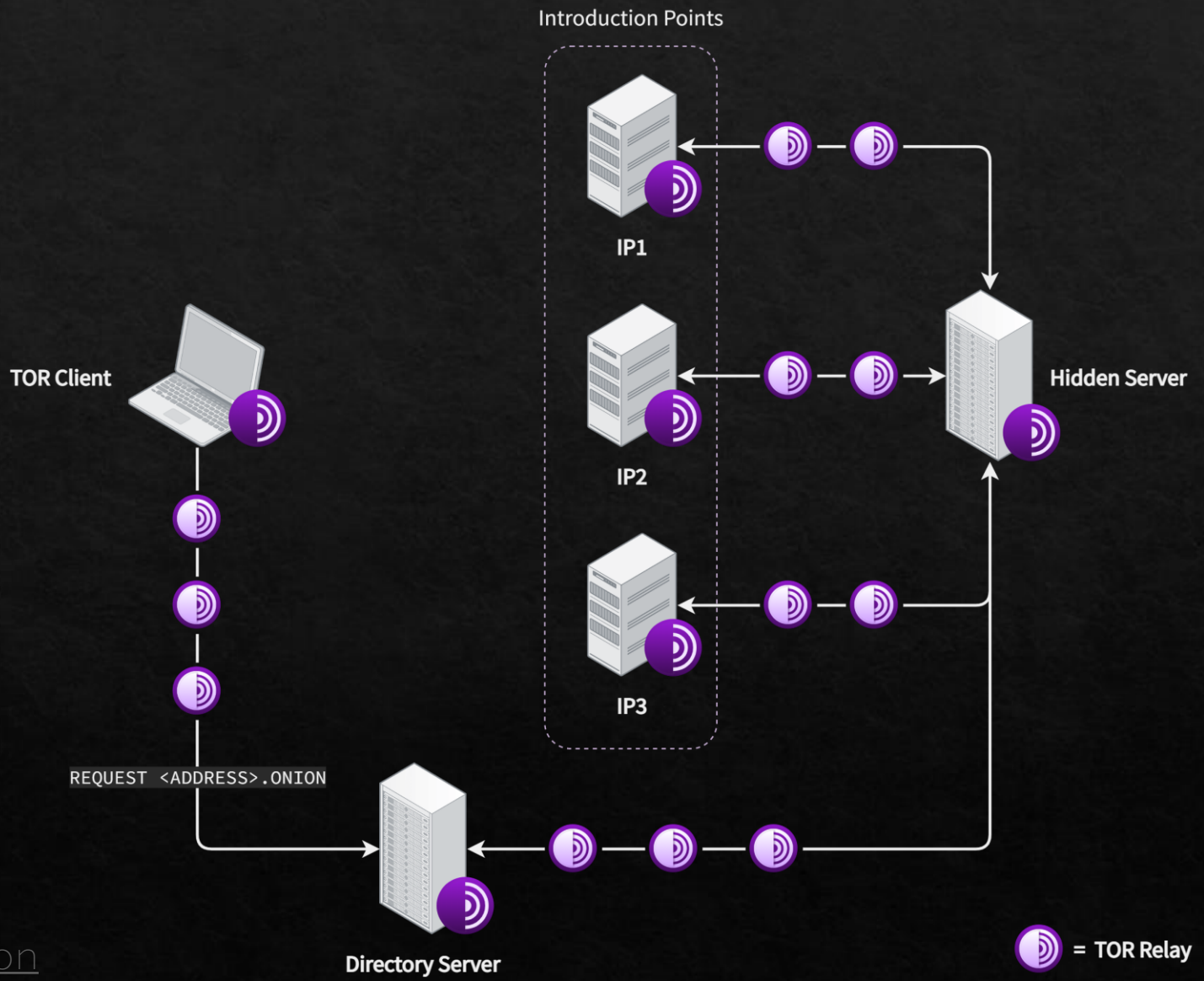
A **Descriptor** contains the address of the three Introduction Points and the servers public key, all signed by the servers' private key.



Hidden Services

General Overview

TOR Client will request a **Directory Server** for information on the requested `.onion` address.



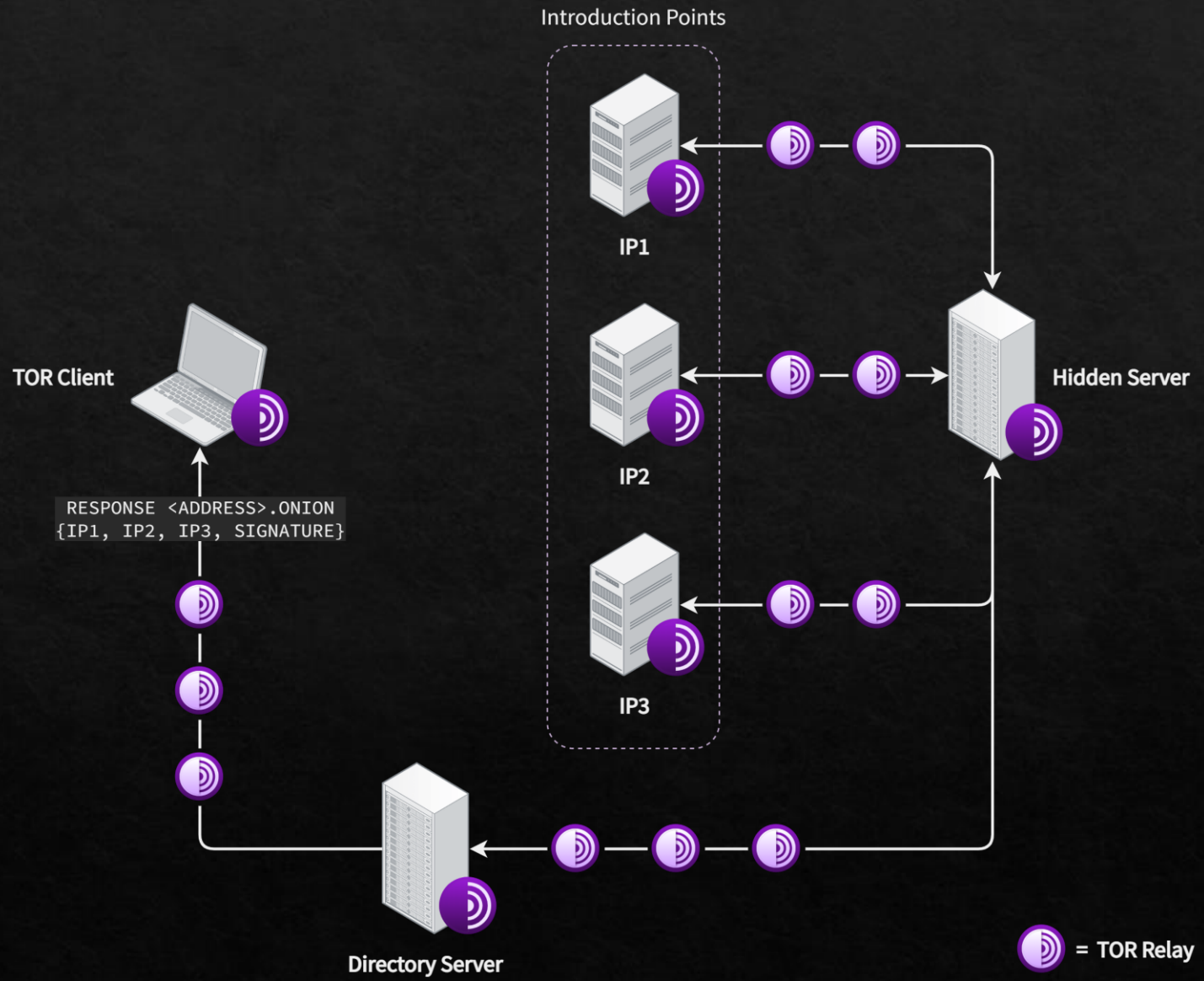
DuckDuckGo's Onion Address:
https://3g2upl4pq6kufc4m.onion

Hidden Services

General Overview

Directory Server will respond to Client with the provided **Descriptor.**

The **Descriptor** contains the IP servers addresses and the public key of the Hidden Server, signed by the servers' private key.

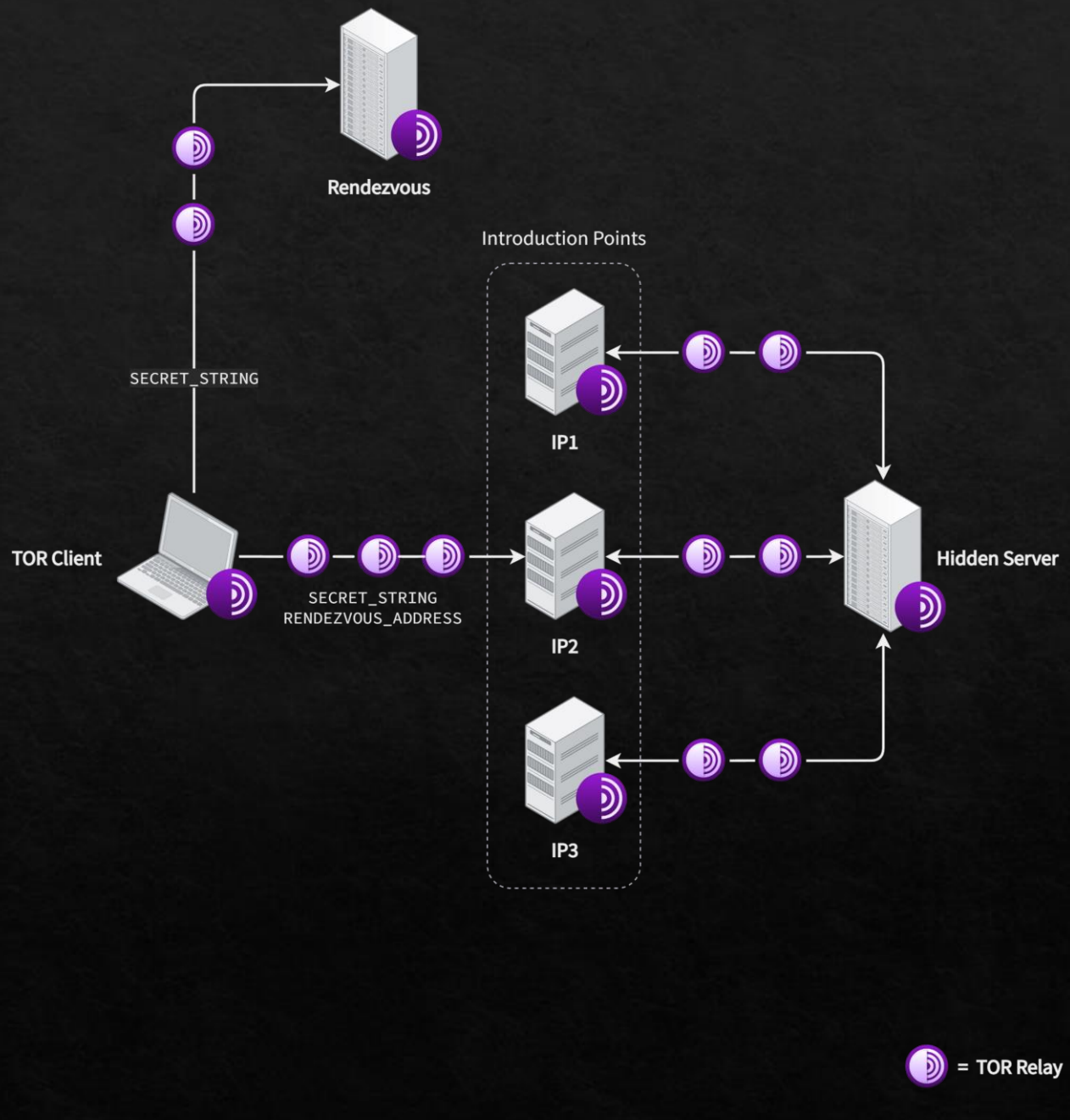


Hidden Services

Technical Overview

TOR Client will send **Introduction Point Server** and **Rendezvous Server** one-time passwords (aka. SECRET_STRING's).

Client will also send Rendezvous Server address to IP server.

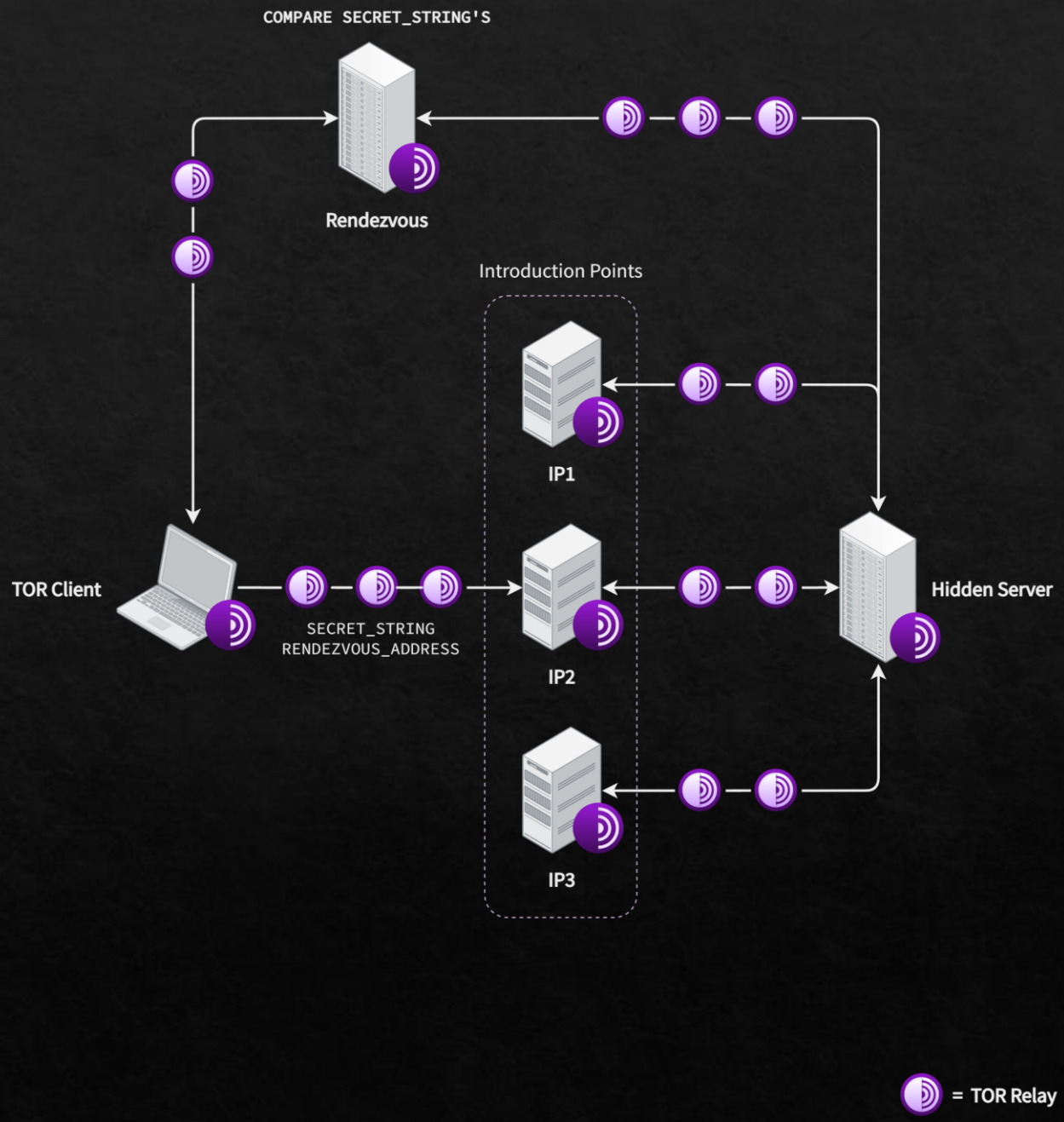


Hidden Services

Technical Overview

Rendezvous Server will compare SECRET_STRING's to confirm server and client identities.

Once confirmed, the relay will connect the client and server, and communication will be performed through the rendezvous server.



Onion Routing

What’s it like today?

Weakness

TOR

- Consensus blocking
- Traffic analysis
- Bad apple attack
- Mouse fingerprinting
- Sniper attack
- Eavesdropping
    - Autonomous system
    - Exit node
    - Internal communication

Strategies of de-anonymize TOR users

Real-world attack carried by government institutions

- User Behavior Analysis
- Passive Traffic Analysis
- Circuit Reconstruction
- Circuit Shaping

Improvement

Exit node vulnerability

- Exit node is compromised
- Be able to acquire the raw data
- Maybe intercepted by the other user or by the router operator
- Solution? SSL/TLS or secure HTTP

SSL/TLS

Secure Sockets Layer / Transport Layer Security

- TLS is successor of SSL
- Cryptographic protocol
- TLS record and handshake protocols
- IETF standard

S-HTTP

Secure Hypertext Transfer Protocol

- HTTPS Alternative
- Only encrypts POST fileds
- Blank headers for URL
- Headers in encrypted payload

Improvement

Timing and traffic analysis

- Hide the path between two computers
- Records of connection between two computers still exist
- Using timing analysis will be able to find the originator and recipients
- Solution? Garlic routing
- Each message is bulb
- I2P calls are garlic cloves

Garlic Routing

Variant of Onion Routing

- Associates with I2P network.
- Encrypts multiple messages together.
- Increased data transfer speed.
- Difficult to track.

References

- Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). **Anonymous connections and onion routing**. IEEE Journal on Selected areas in Communications, 16(4), 482-494.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). **Tor: The second-generation onion router**. Naval Research Lab Washington DC.
- **How do Onion Services work?.** Tor Project. Accessed 13/04/2022. Available at: https://community.torproject.org/onion-services/overview/
- **World Wide Browser Usage**. Statista. Accessed 13/04/2022. Available at: https://www.statista.com/statistics/543218/worldwide-internet-users-by-browser
- **Tor User Metrics**. The TOR Project. Accessed 13/04/2022. Available at: https://metrics.torproject.org/userstats-relay-country.html
- Moore, D. & Rid, T. (2016). **Cryptopolitik and the Darknet**. Global Politics and Strategy, 58. https://doi.org/10.1080/00396338.2016.1142085
- **Garlic Routing and "Garlic" Terminology.** I2P Team. Accessed 12/04/2022. Available at: https://geti2p.net/en/docs/how/garlic-routing
- Rescorla, E., Schiffman, A. (1996). **The Secure HyperText Transfer Protocol.** Accessed 12/04/2022. Available at: https://datatracker.ietf.org/doc/html/draft-ietf-wts-shttp-01.txt
- **Attacks on the Tor Network to de-anonymize Tor users.** Arun KL. Accessed 12/04/2022. Available at: https://thesecmaster.com/4-types-of-attacks-on-the-tor-network-to-de-anonymize-tor-users/
- **The Invisible Internet Project**. I2P Team. Accessed 12/04/2022. Available at: https://geti2p.net/en/