Introduction to Tor

Secure Web Browsing and Anonymity

Sukhbir Singh
sukhbir@torproject.org

October 29, 2017

Before We Begin...

Before We Begin...

- Understand your threat model

Before We Begin...

- Understand your threat model
- If in doubt, it's better to ask

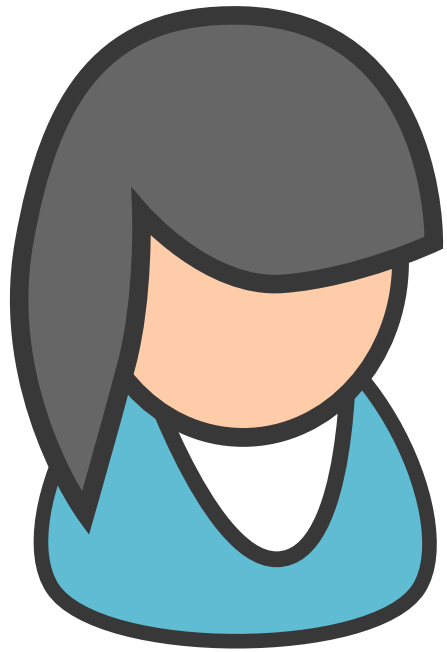
Before We Begin...

- Understand your threat model
- If in doubt, it's better to ask
- Respect the group and the discussions

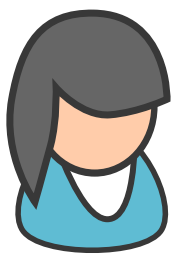
Before We Begin...

- Understand your threat model
- If in doubt, it's better to ask
- Respect the group and the discussions
- No photographs please

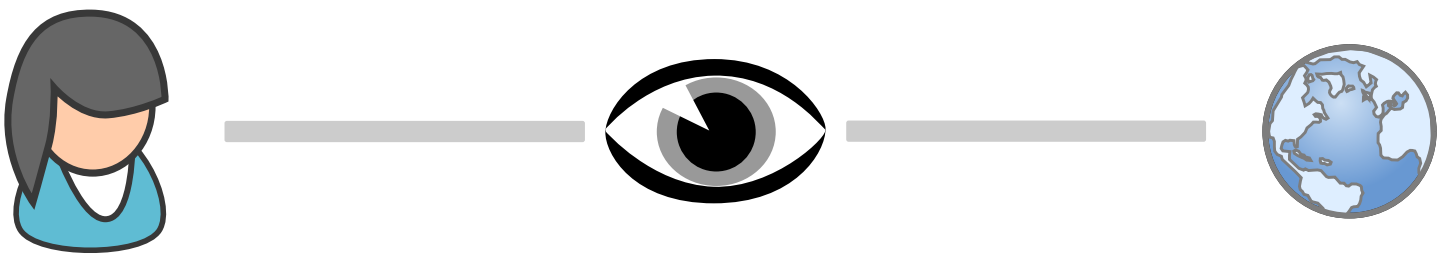
Anonymity on the Internet



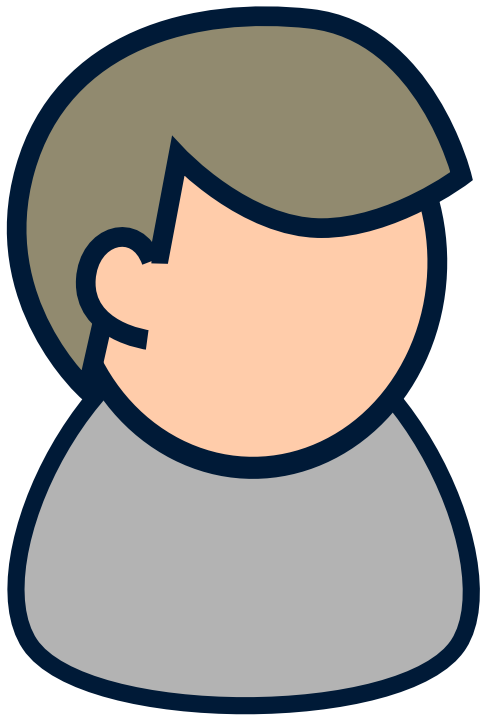
Anonymity on the Internet



Anonymity on the Internet

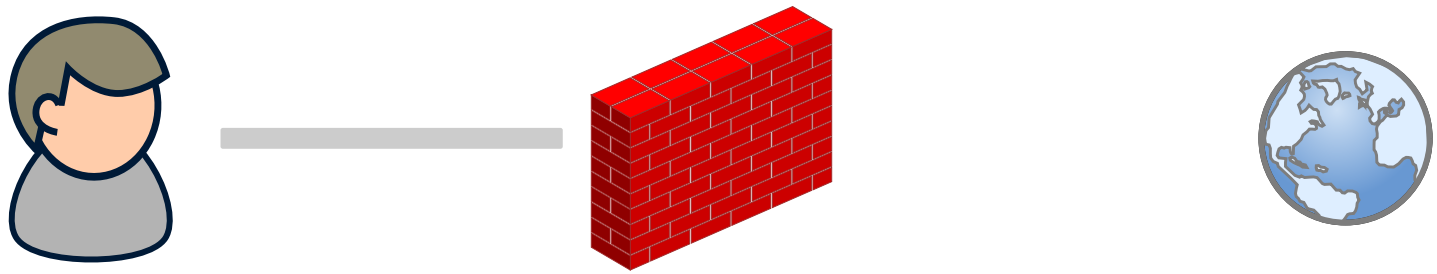


Anonymity on the Internet

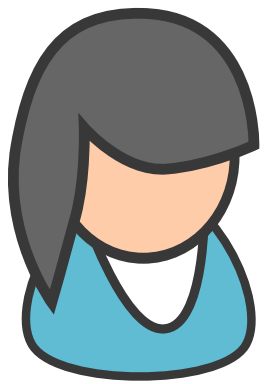


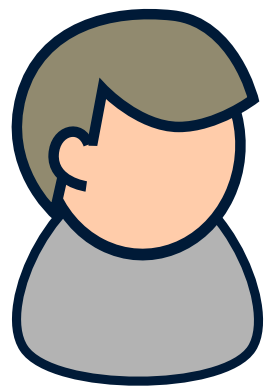
Anonymity on the Internet

Anonymity on the Internet



Anonymity on the Internet





Anonymity on the Internet

“On the Internet, Nobody Knows...”

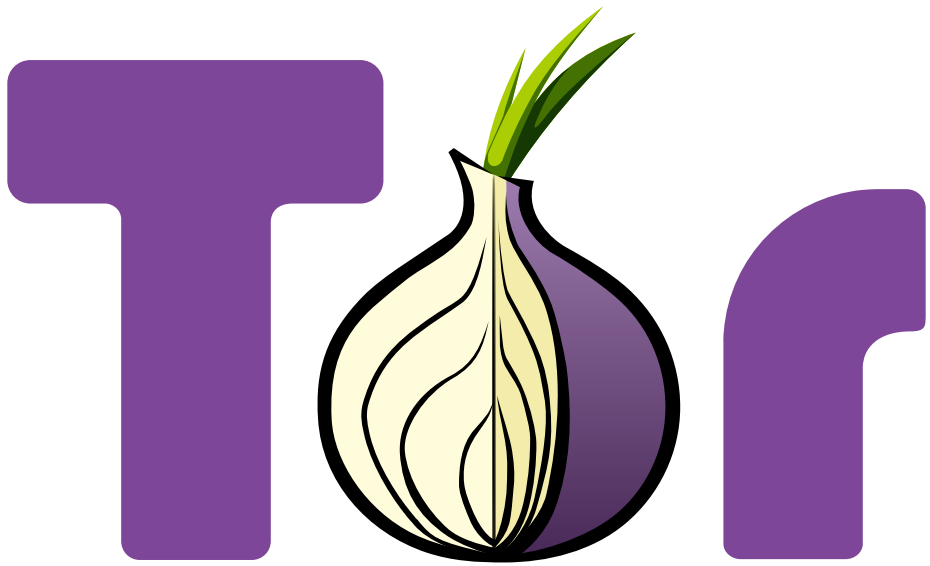
"On the Internet, nobody knows you're a dog."

†

† Image from The New Yorker cartoon by Peter Steiner, 1993

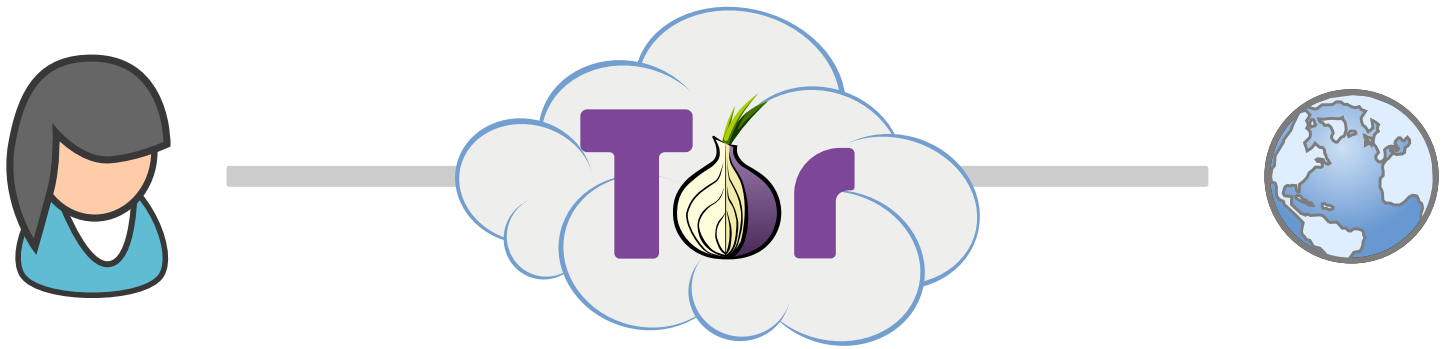
On the Internet, *They* Know...

Tor: The Onion Router

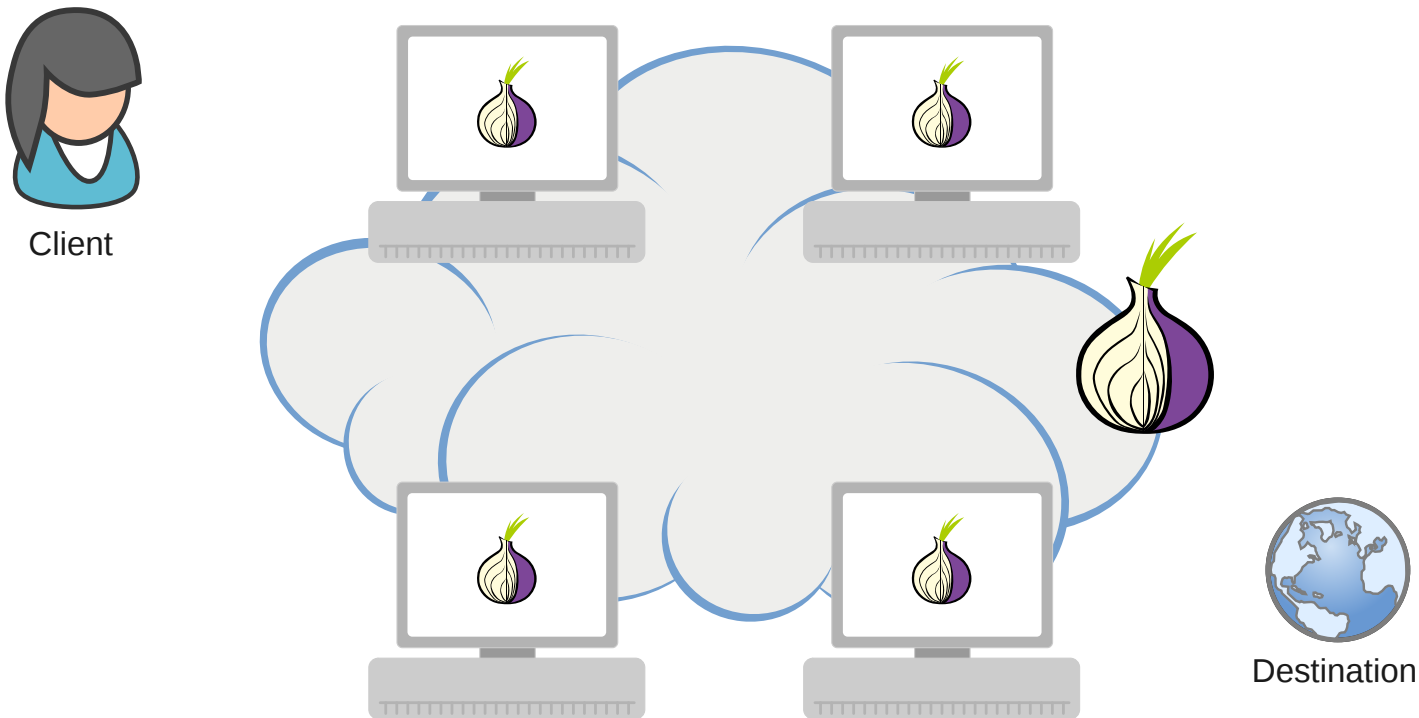


Tor: The Onion Router

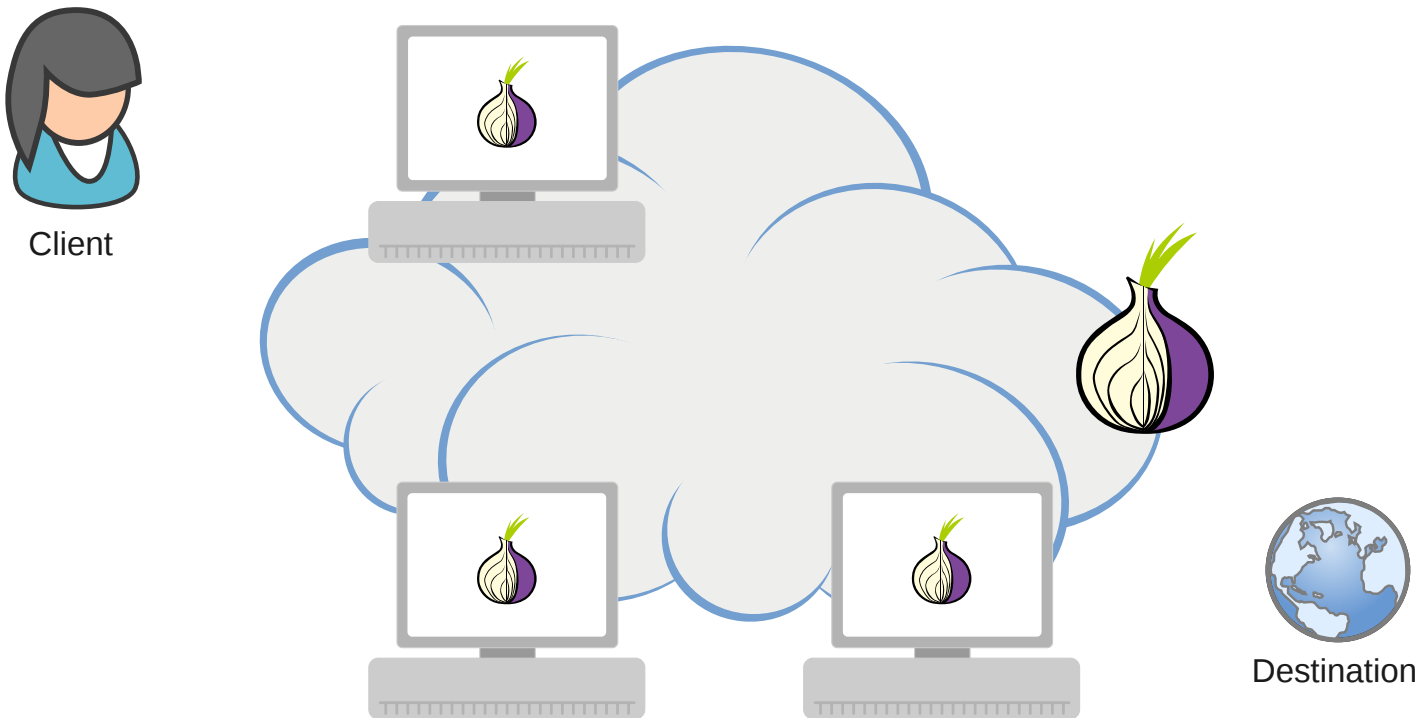
Tor: The Onion Router



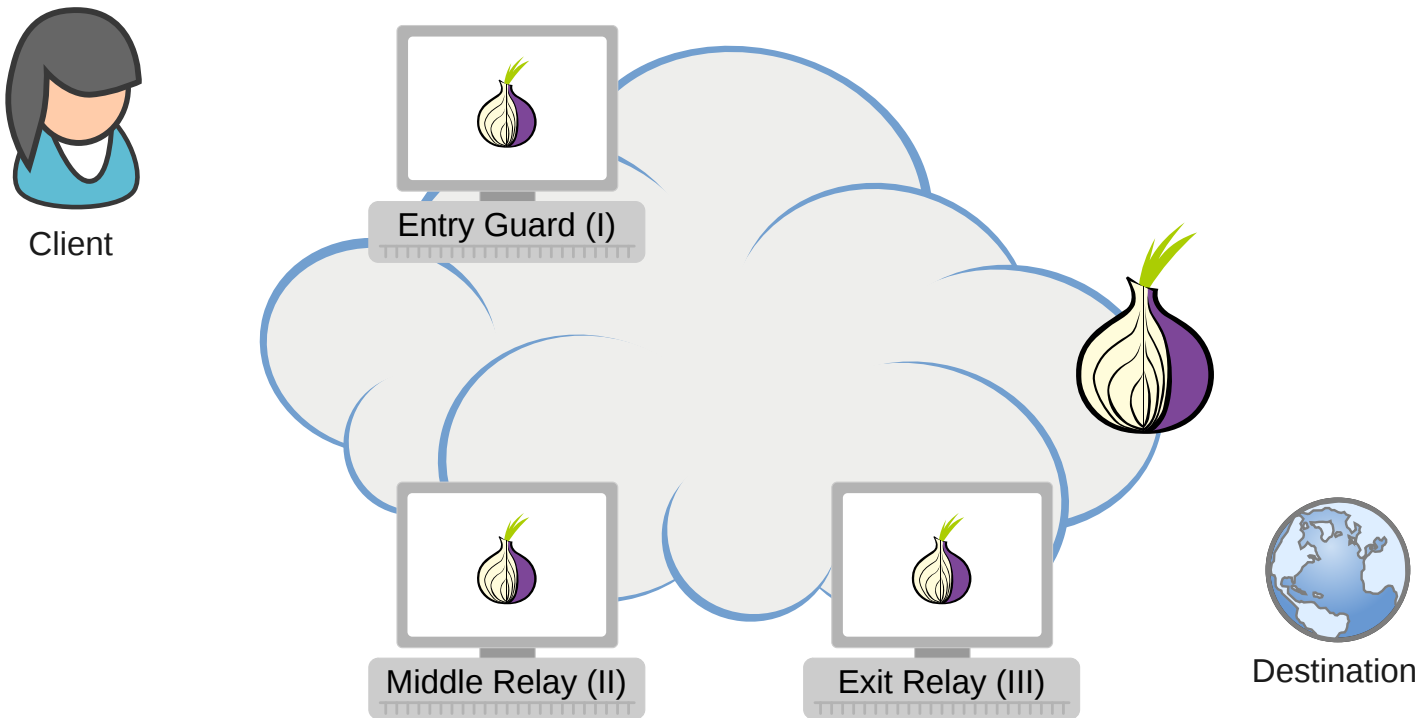
Tor: The Onion Router



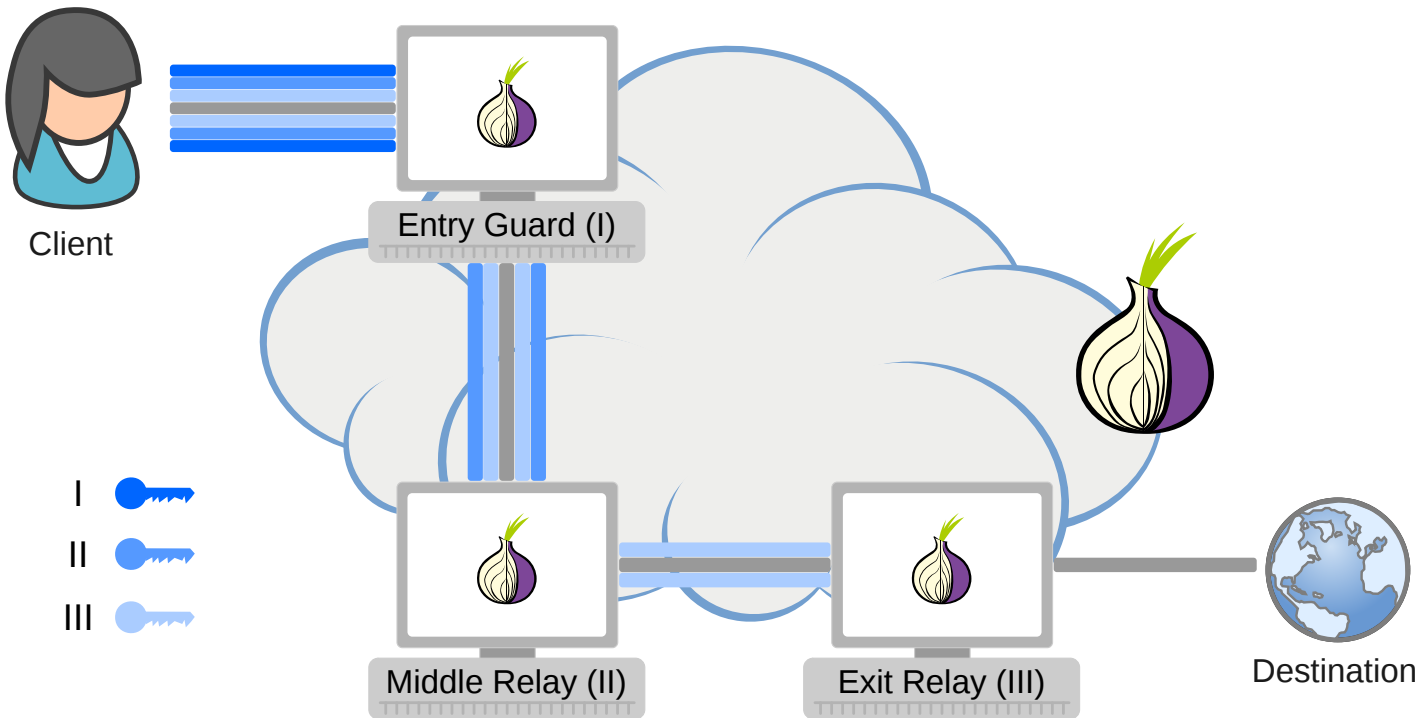
Tor: The Onion Router



Tor: The Onion Router

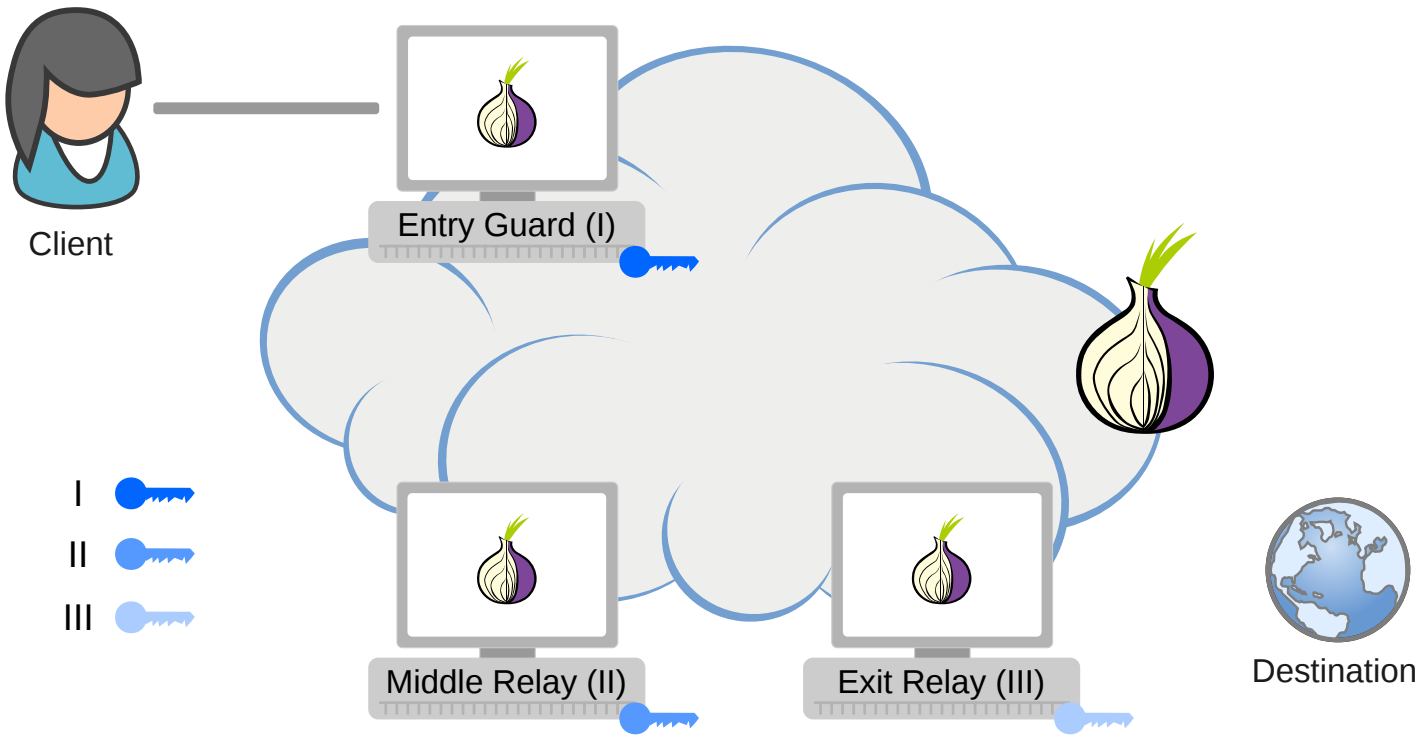


Tor: The Onion Router

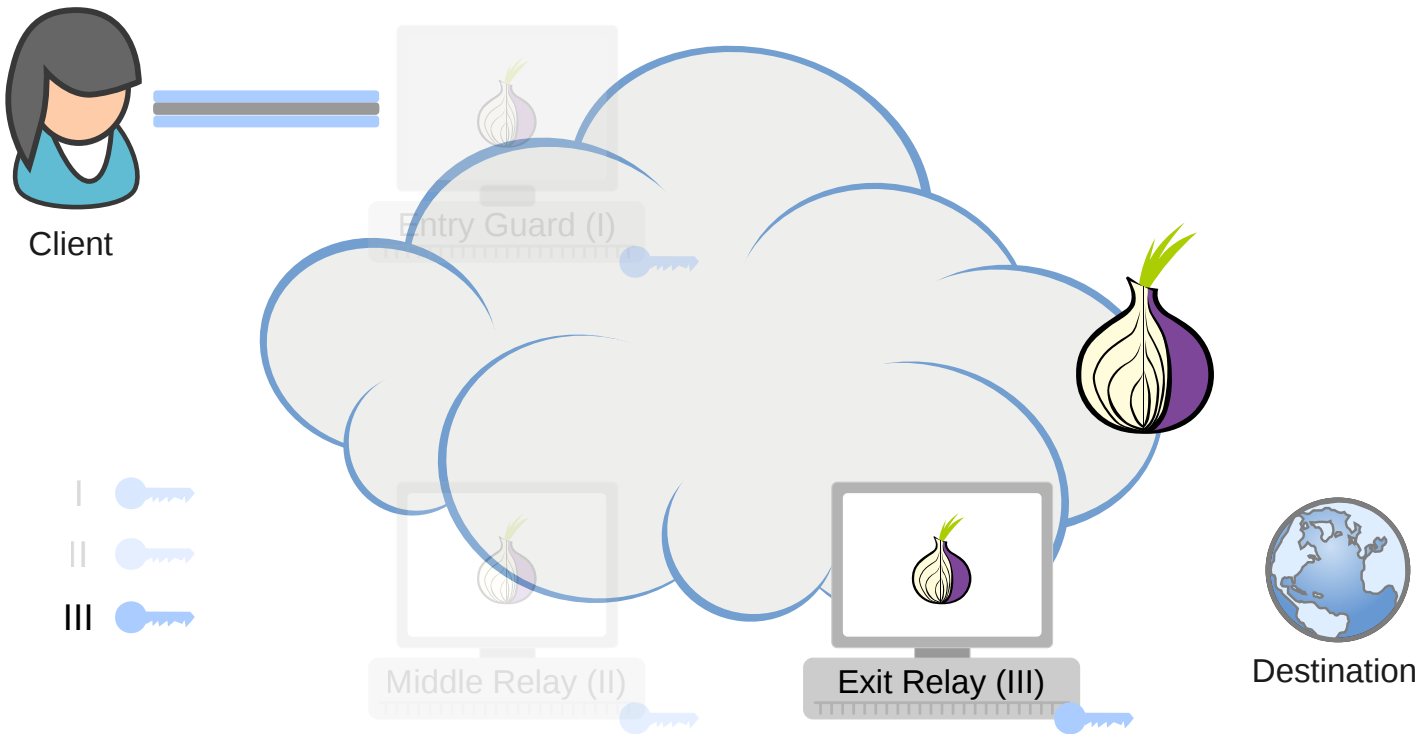


Tor: The Onion Router

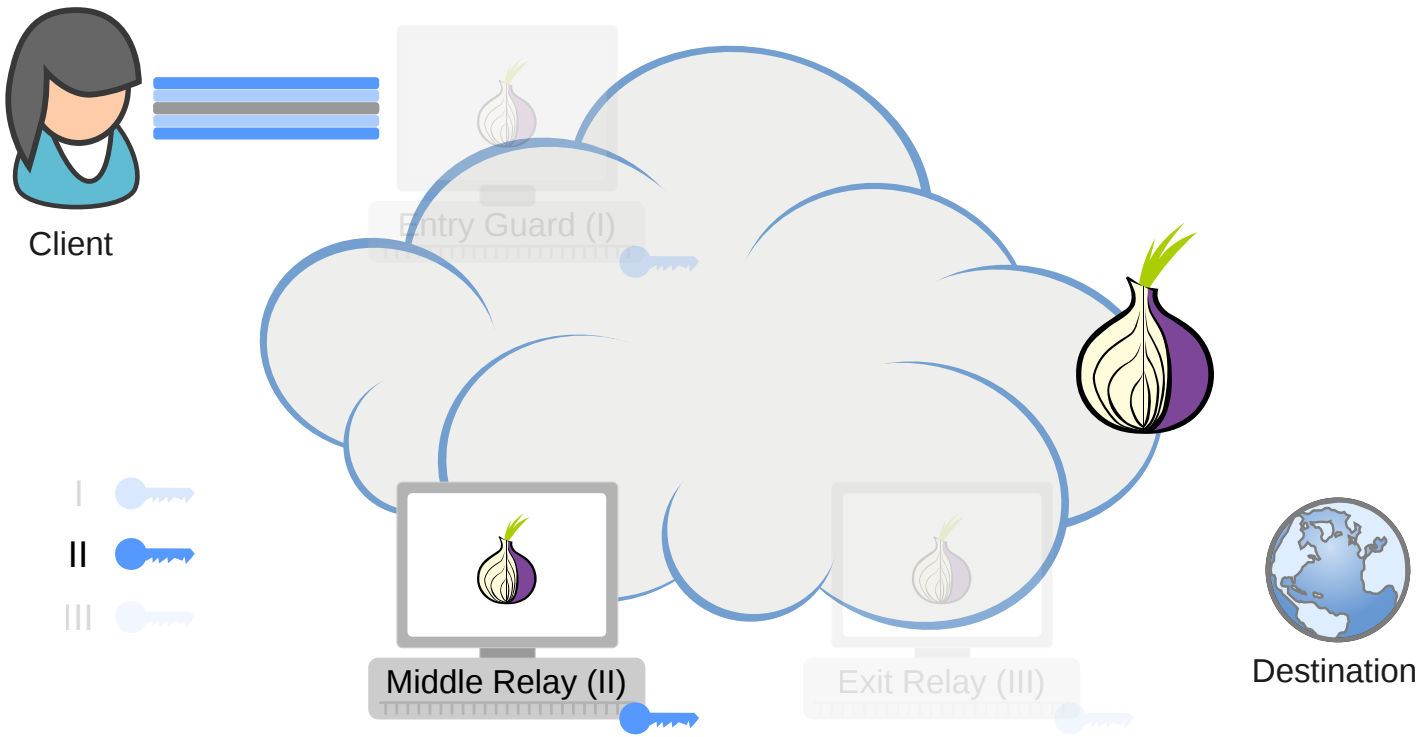
Tor: The Onion Router



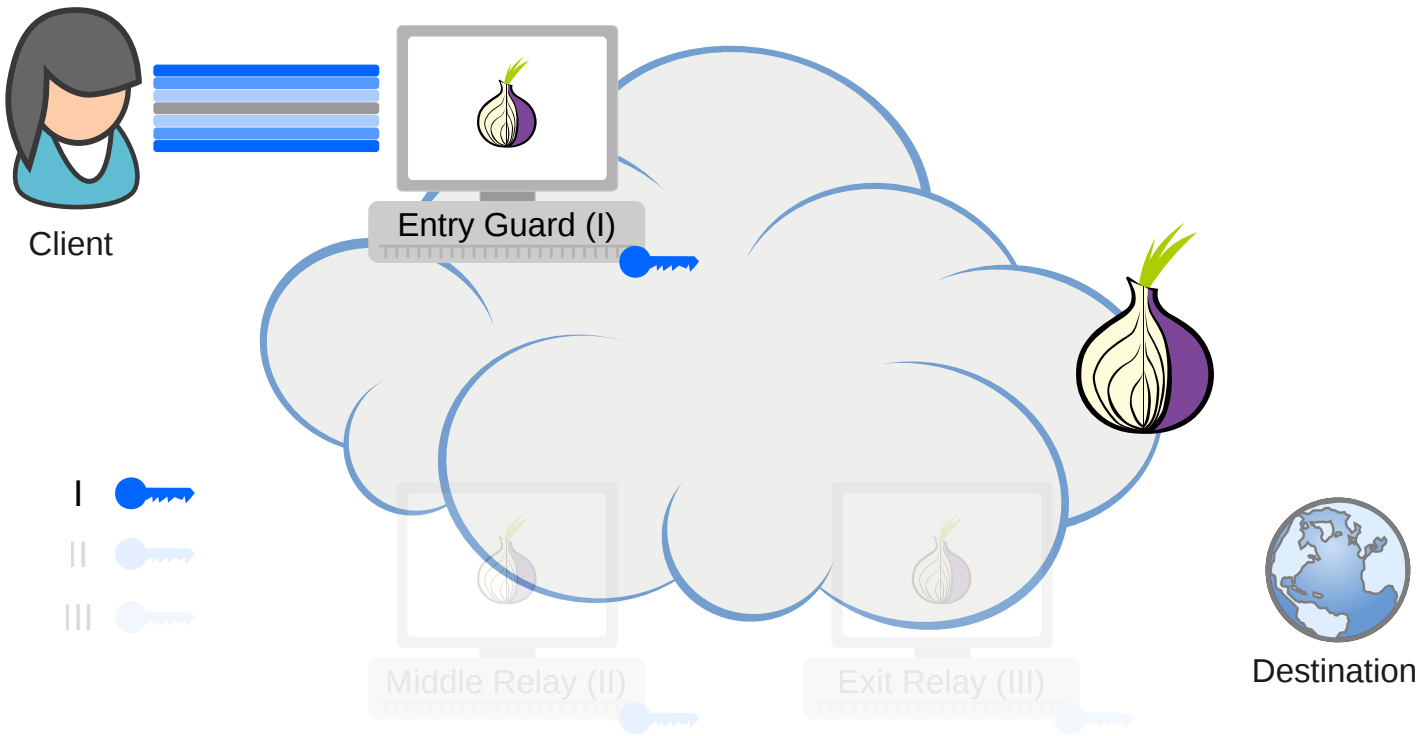
Tor: The Onion Router



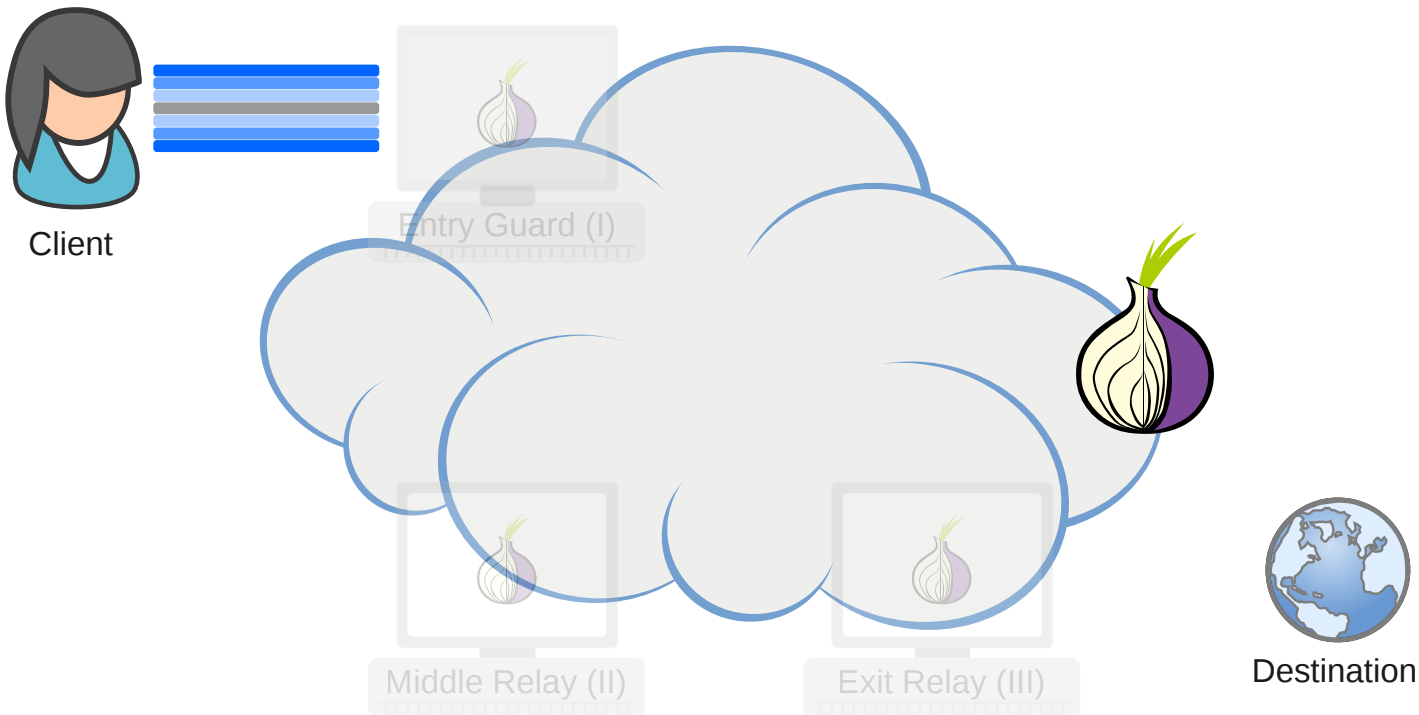
Tor: The Onion Router



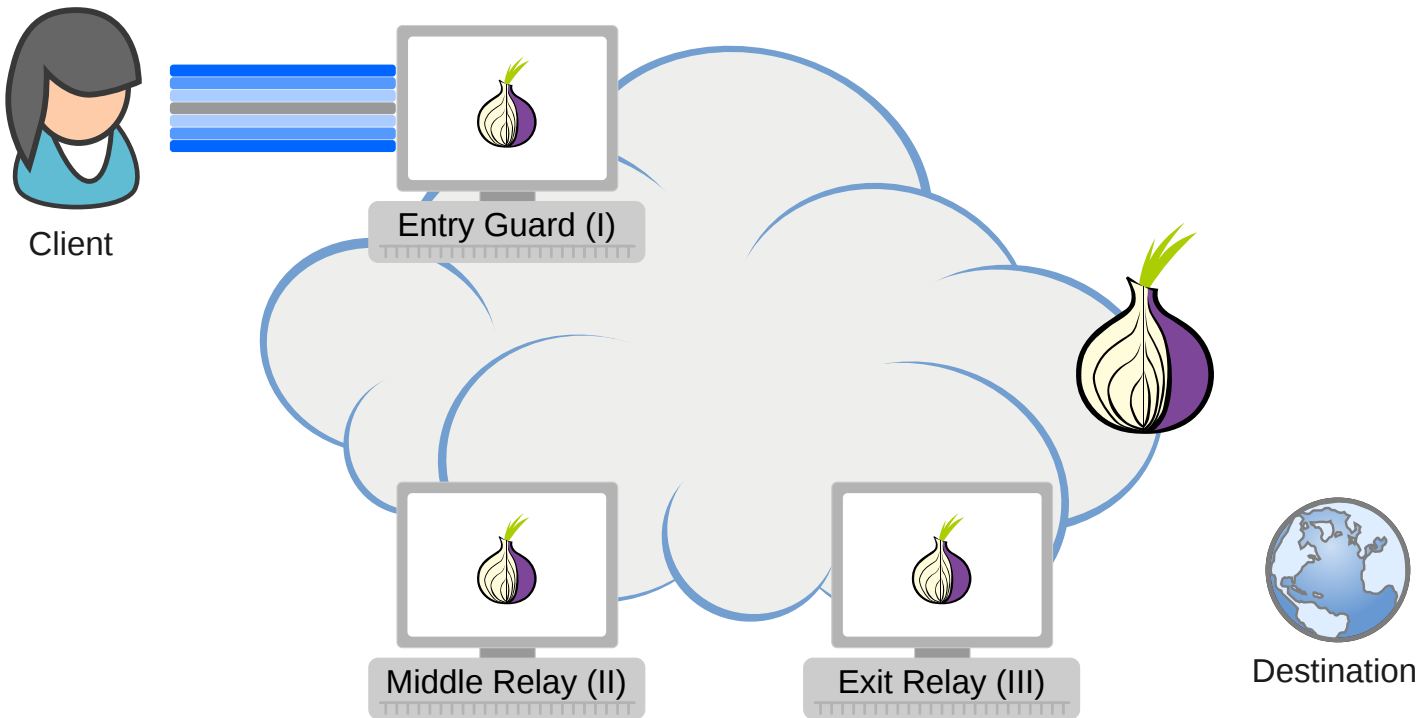
Tor: The Onion Router



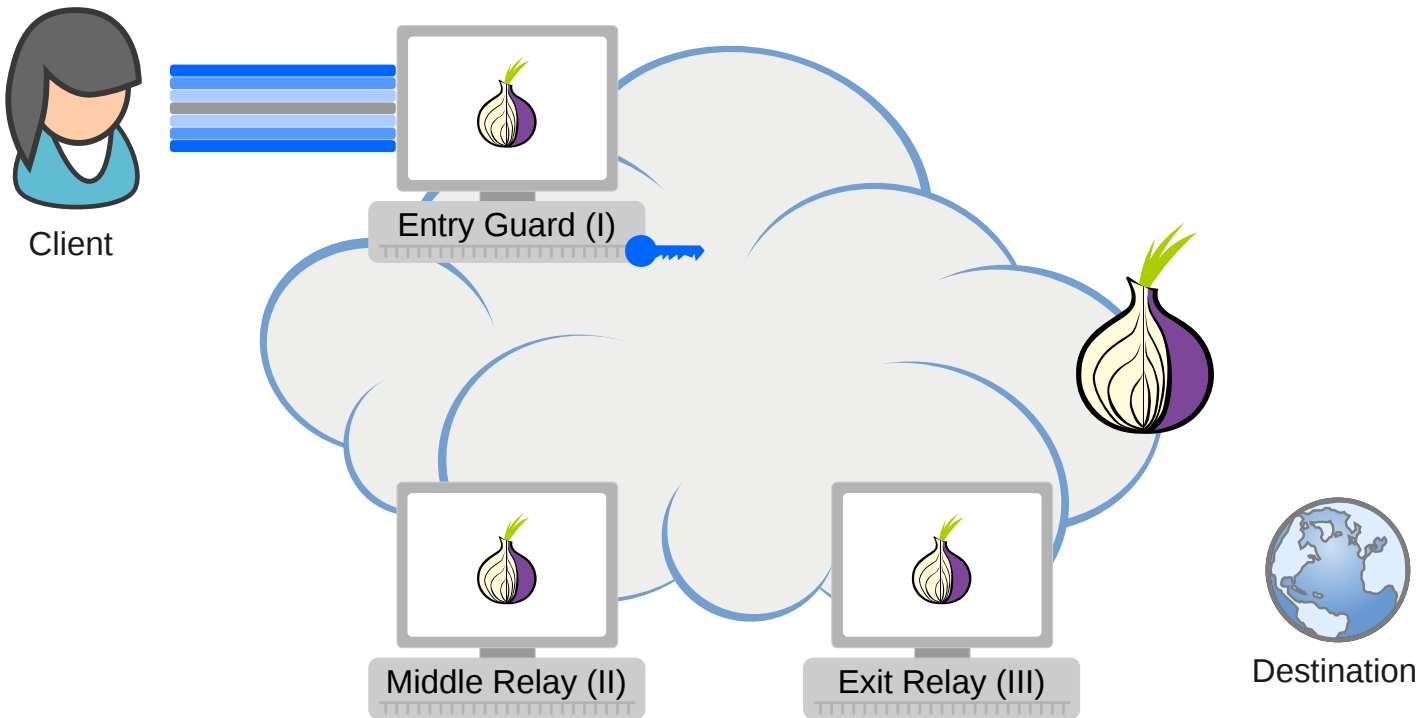
Tor: The Onion Router



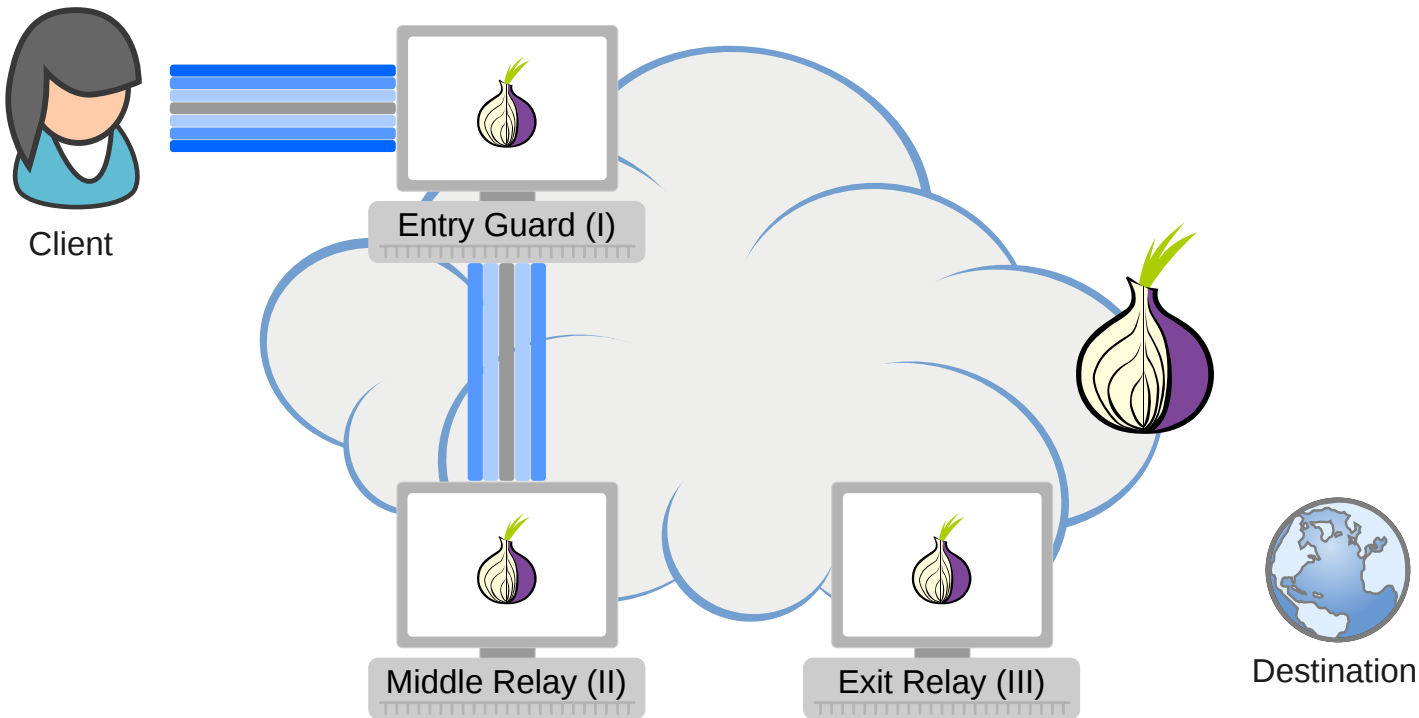
Tor: The Onion Router



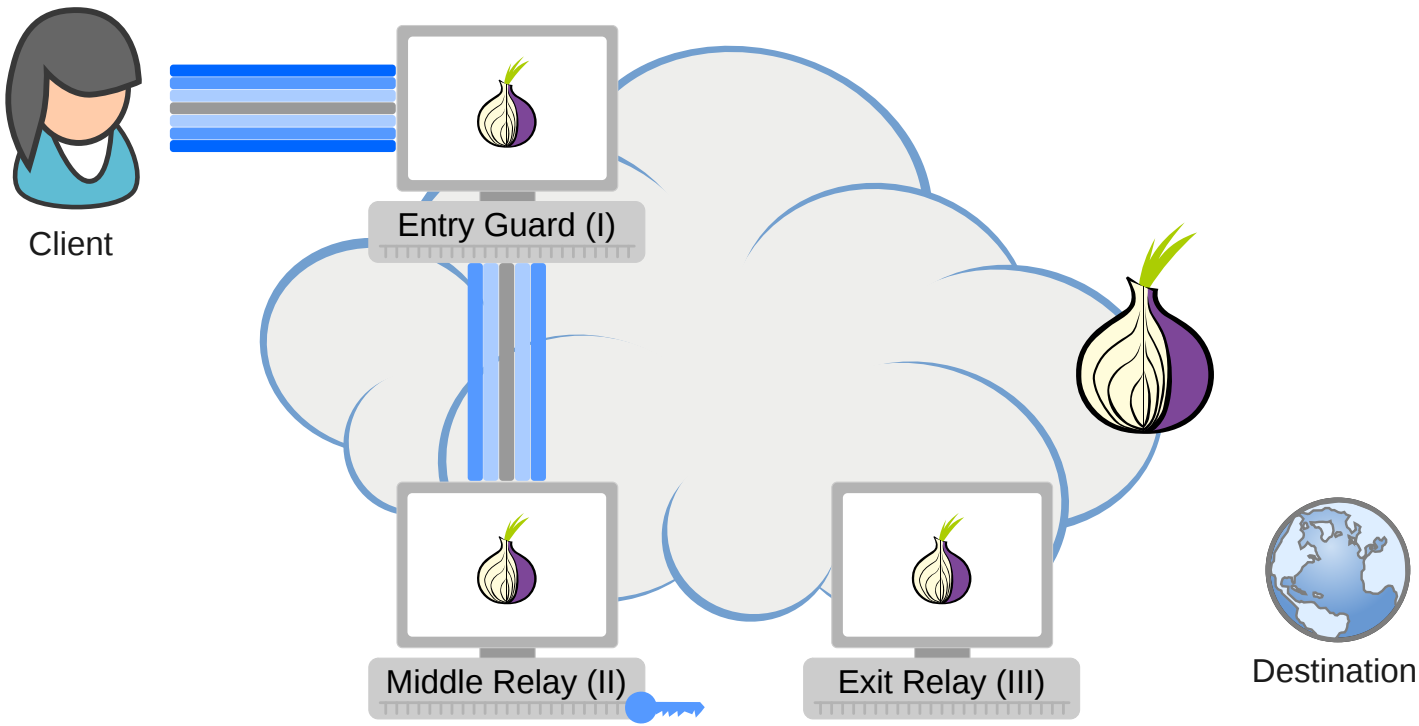
Tor: The Onion Router



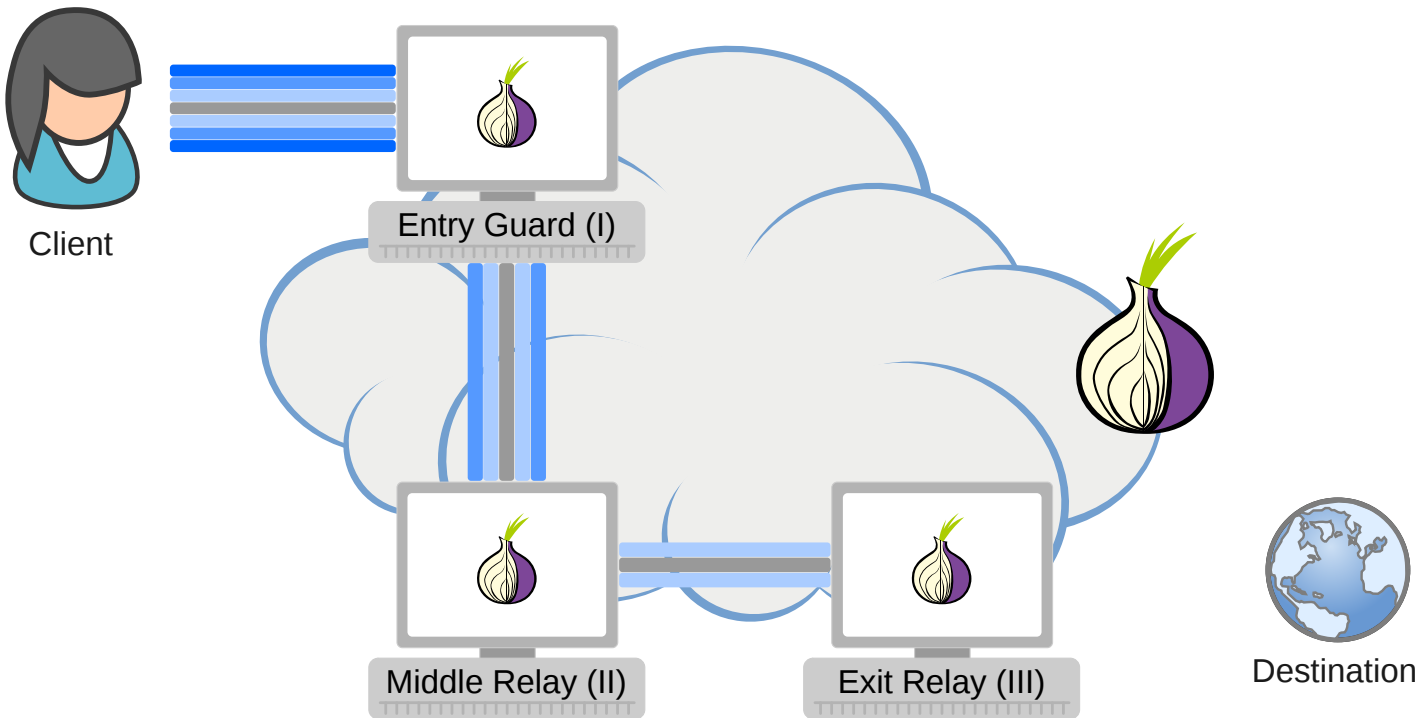
Tor: The Onion Router



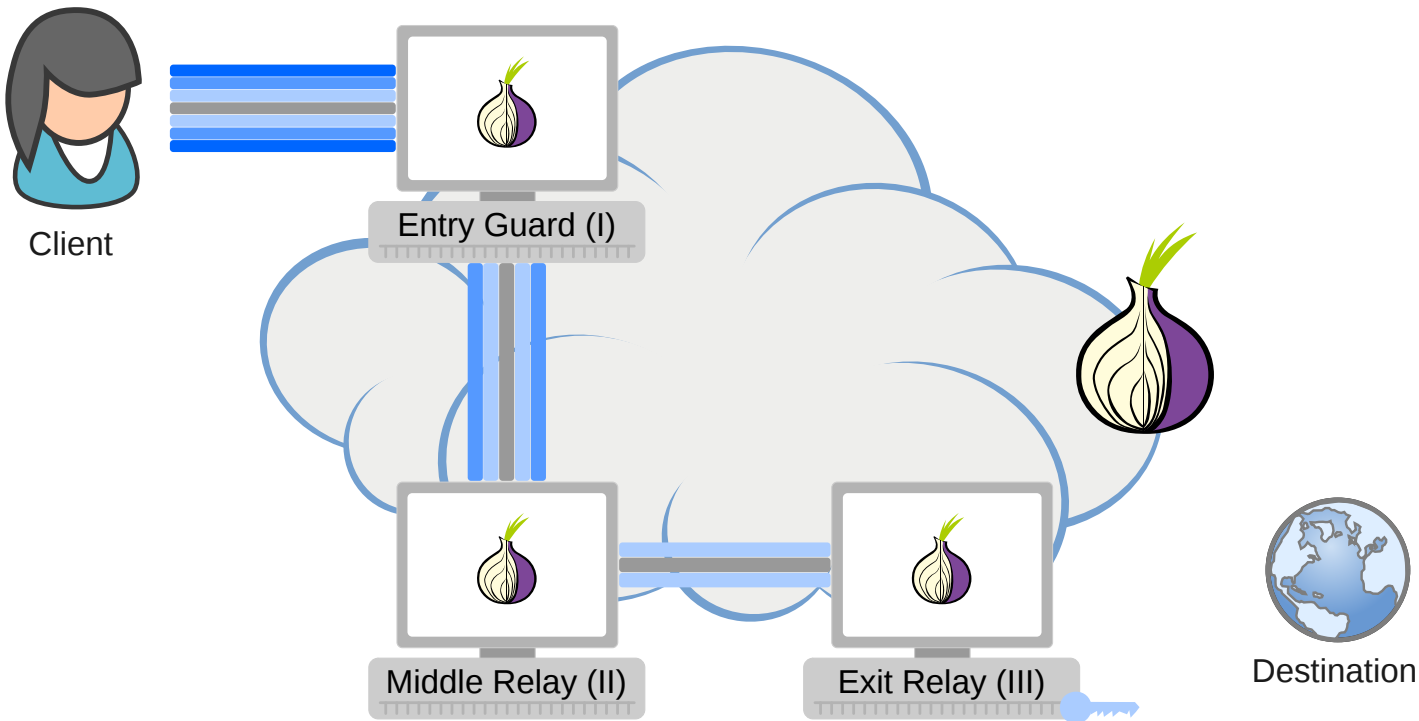
Tor: The Onion Router



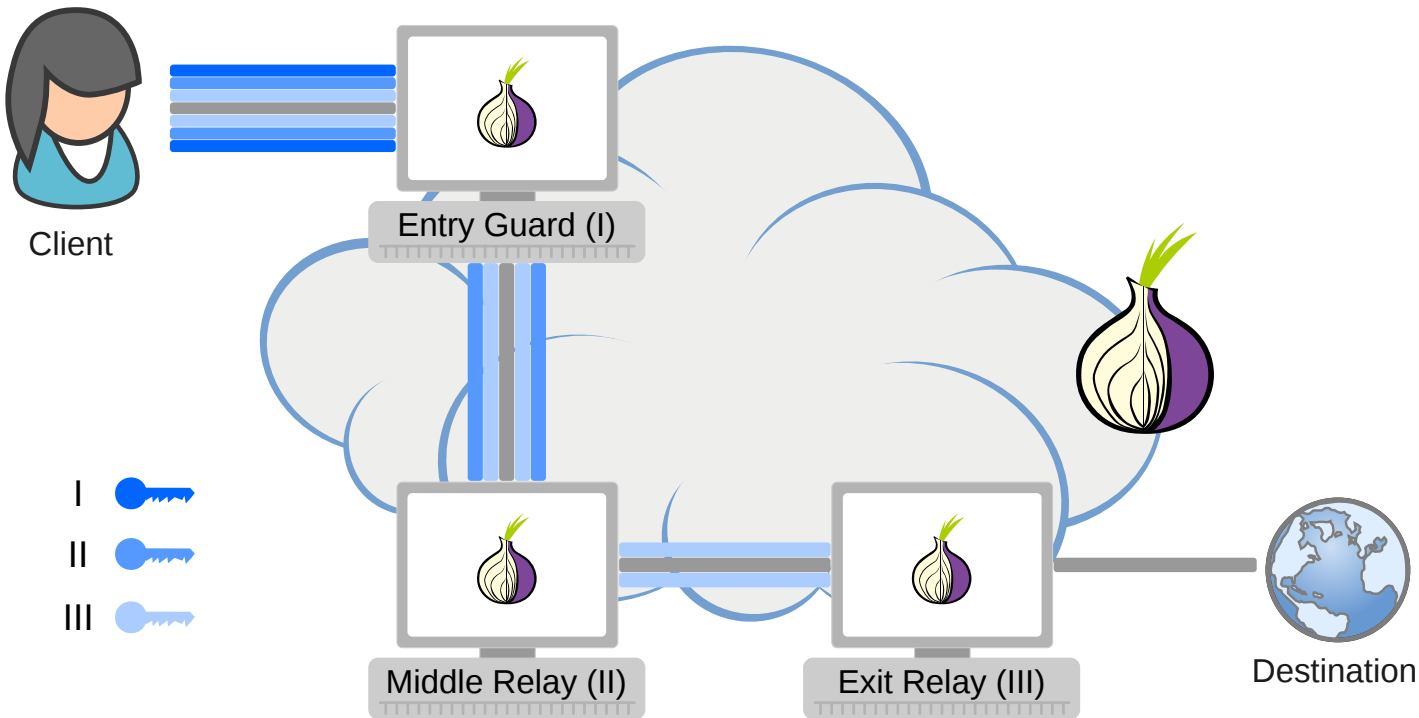
Tor: The Onion Router



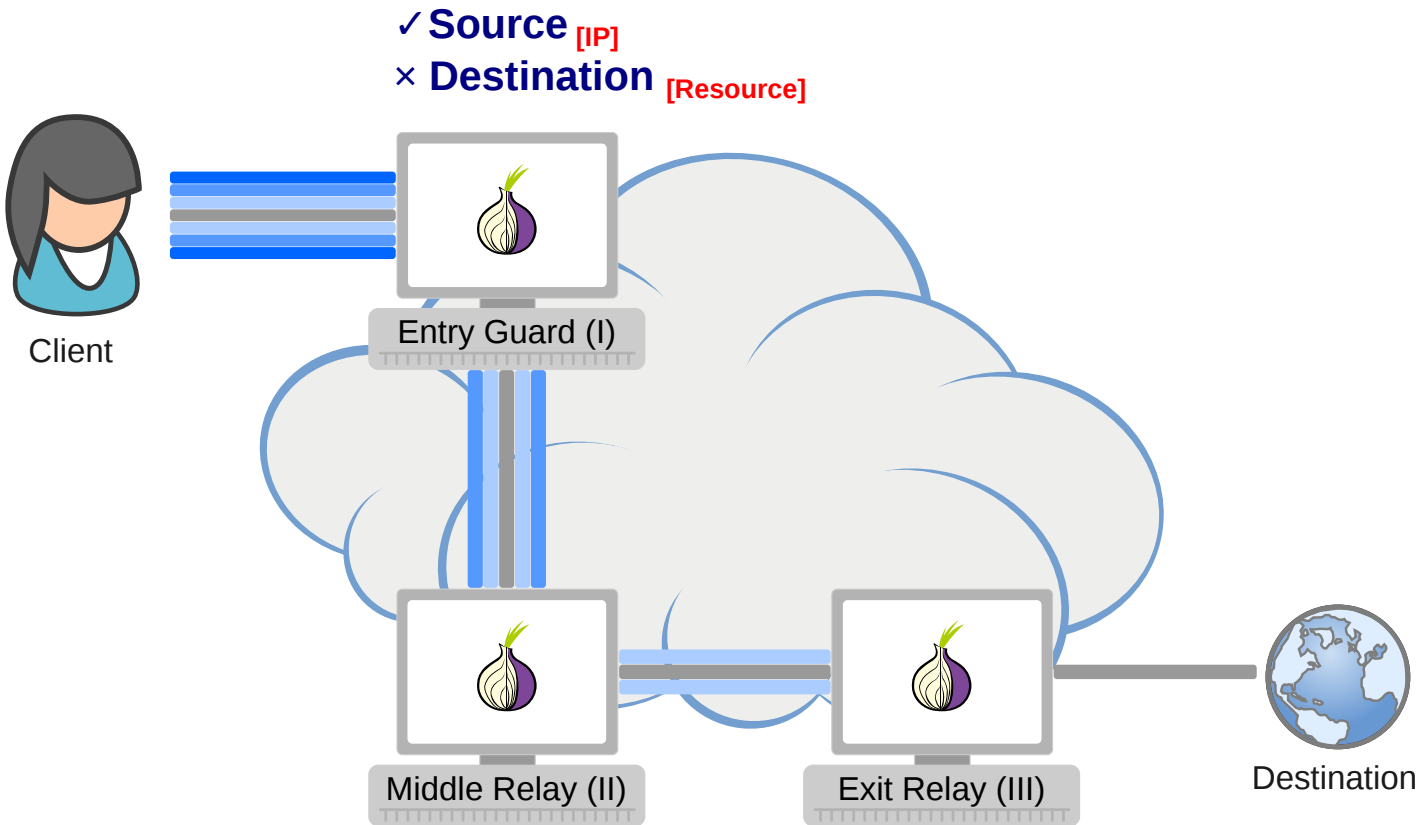
Tor: The Onion Router



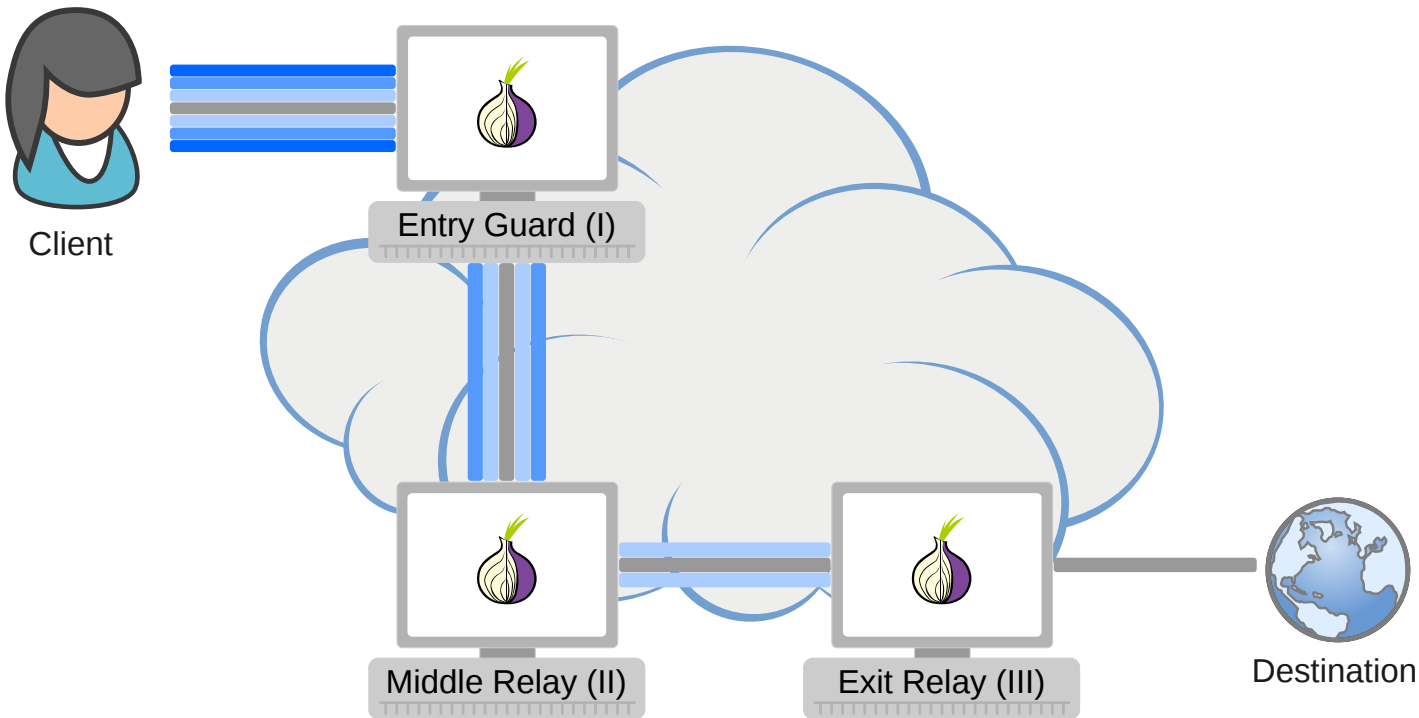
Tor: The Onion Router



Tor: The Onion Router



Tor: The Onion Router



× **Source** [IP]
✓ **Destination** [Resource]

Tor: The Onion Router

- Low-latency anonymity

*https://metrics.torproject.org

Tor: The Onion Router

- Low-latency anonymity
- Distributed design

*https://metrics.torproject.org

Tor: The Onion Router

- Low-latency anonymity
- Distributed design
- 2,000,000 users and 6000 relays
  - 100 Gbit/sec available bandwidth

*https://metrics.torproject.org

Who Uses Tor?

Who Uses Tor?

- Journalists

Who Uses Tor?

- Journalists
- Activists

Who Uses Tor?

- Journalists
- Activists
- You...

little-t-tor

little-t-tor

- Core of the Tor software ecosystem

little-t-tor

- Core of the Tor software ecosystem
- Runs as a daemon and sets up a local SOCKS5 proxy

little-t-tor

- Core of the Tor software ecosystem
- Runs as a daemon and sets up a local `SOCKS5` proxy
- But there are still application-level concerns. . .

Tor Browser

Tor (`little-t-tor`)

+

Mozilla Firefox (Modified ESR)

Tor Browser: Demo

Download from

https://www.torproject.org/torbrowser

Staying Safe

Staying Safe

- Use Tor Browser

Staying Safe

- Use Tor Browser
- Be careful when opening downloaded documents

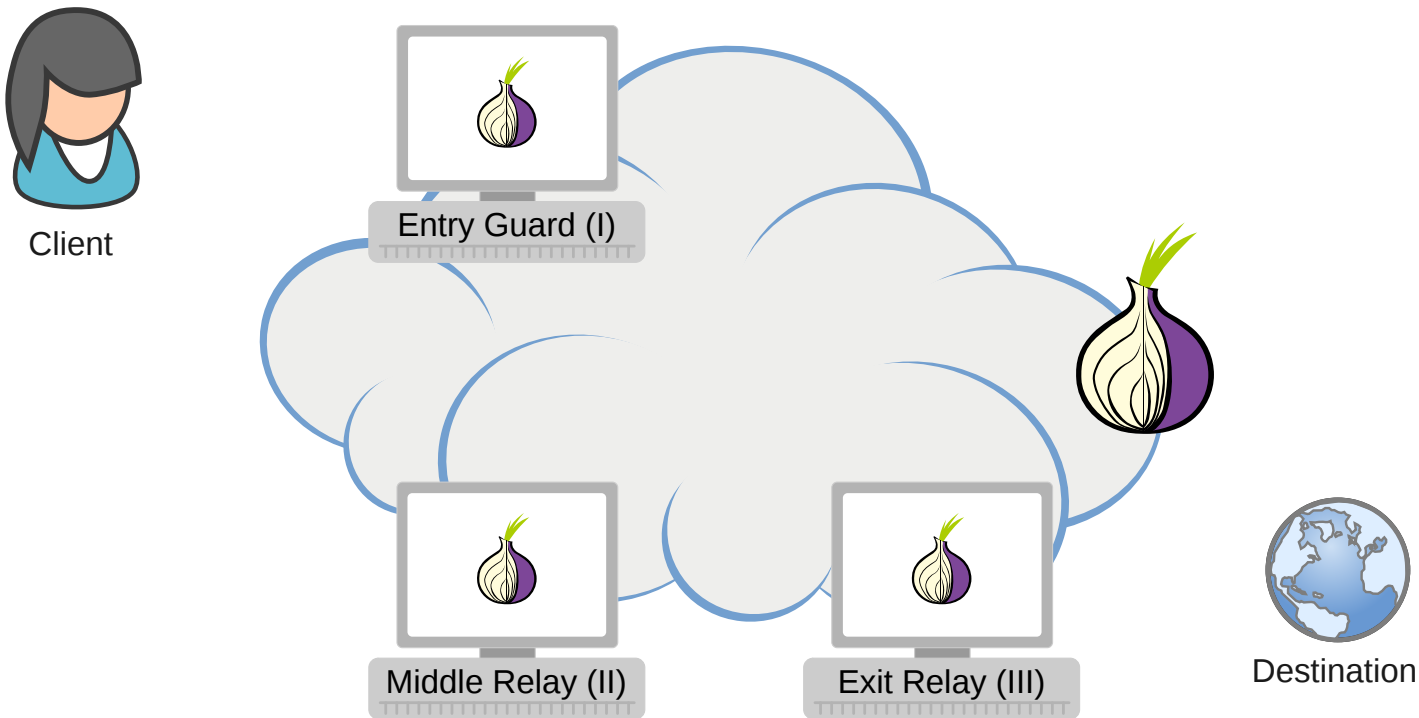
Staying Safe

- Use Tor Browser
- Be careful when opening downloaded documents
- Use HTTPS versions of websites

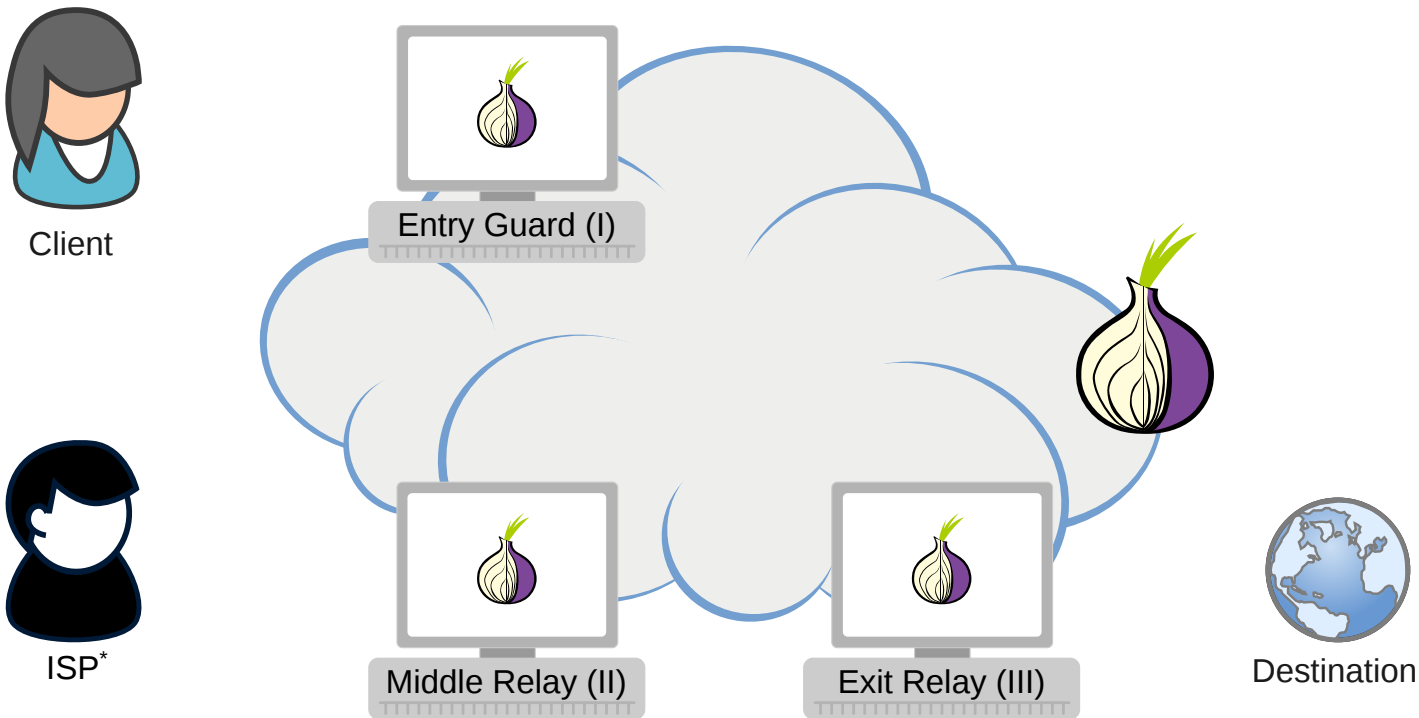
Staying Safe

- Use Tor Browser
- Be careful when opening downloaded documents
- Use HTTPS versions of websites
- Don't enable or install browser plugins

How Governments Censor Tor

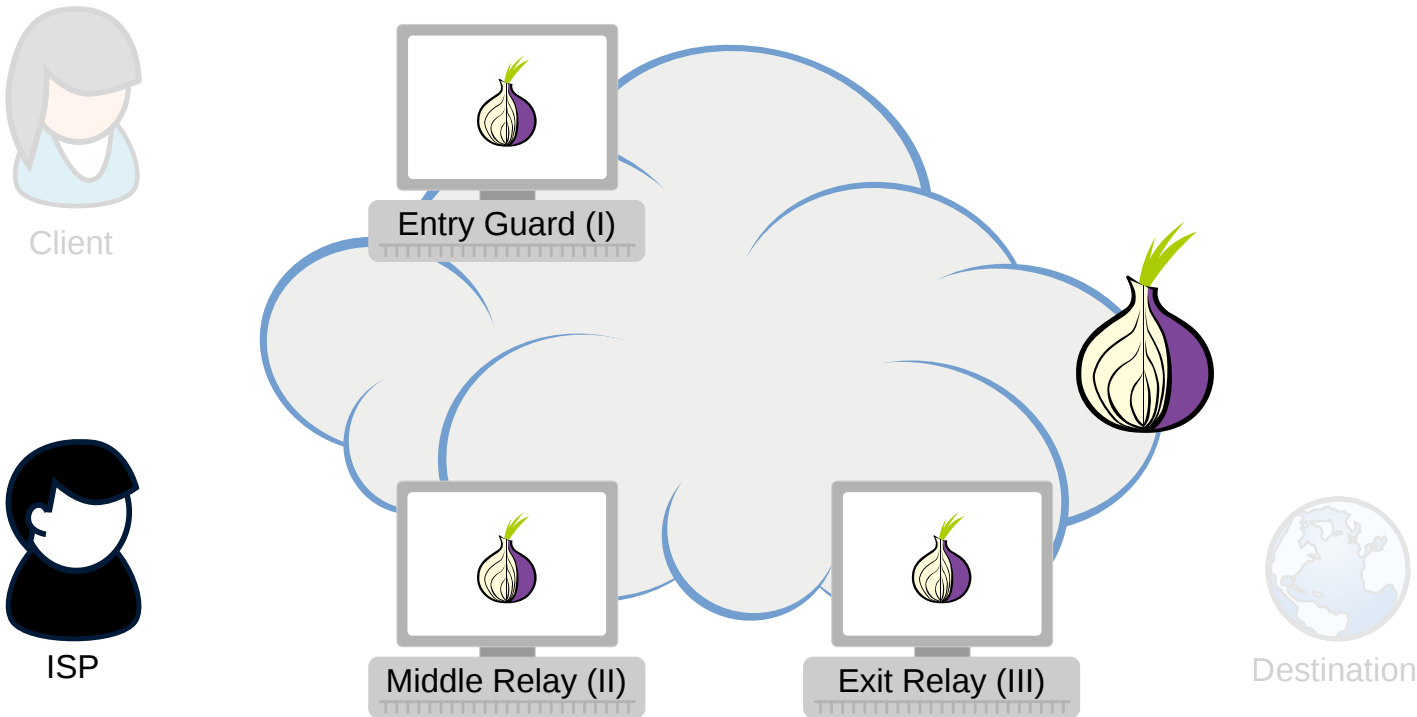


How Governments Censor Tor

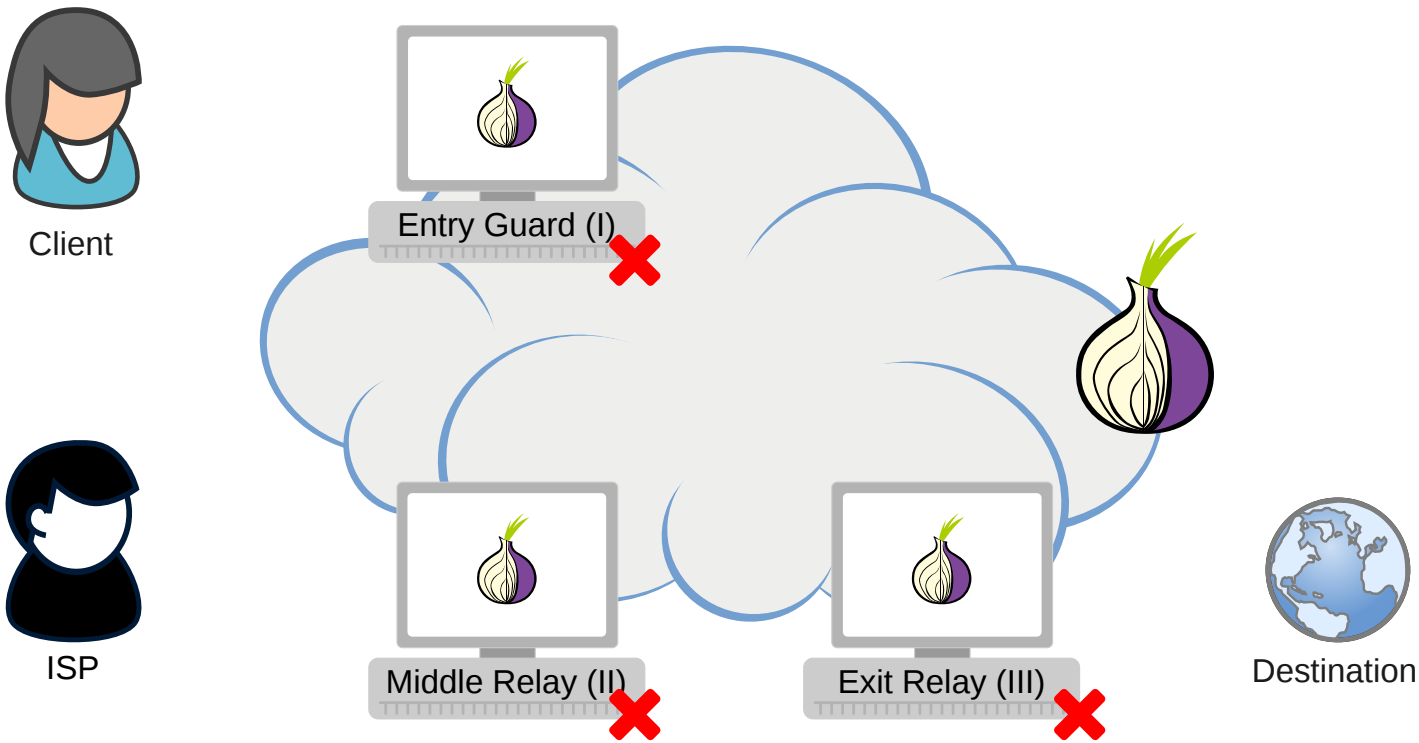


* - government

How Governments Censor Tor



How Governments Censor Tor



Tor Bridges

Tor Bridges

- If using Tor is
  - blocked by censorship
  - dangerous or considered supicious

Tor Bridges

- If using Tor is
  - blocked by censorship
  - dangerous or considered supicious
- Then you need to use a *bridge*

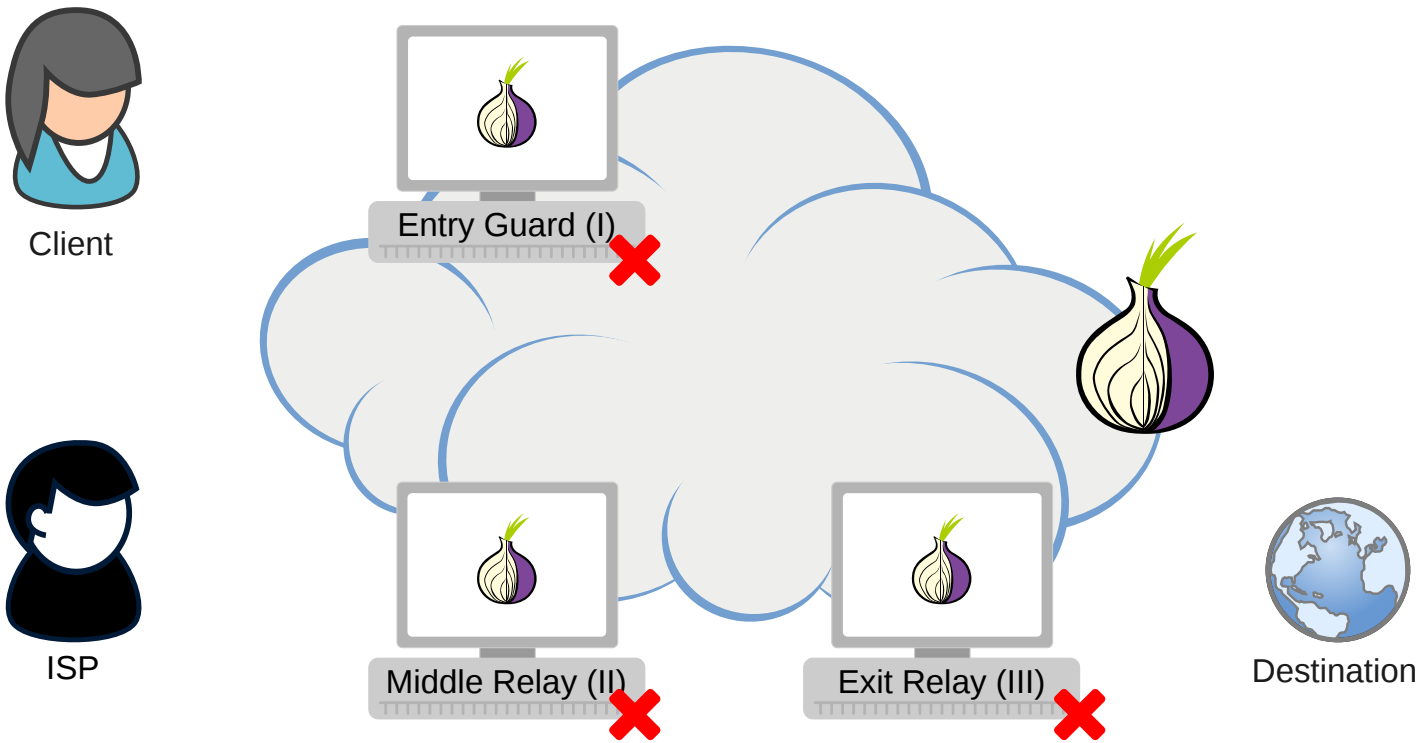
Tor Bridges

- If using Tor is
  - blocked by censorship
  - dangerous or considered supicious
- Then you need to use a *bridge*
  - an alternative entry point to the network
  - makes it harder for your ISP to know that you are using Tor

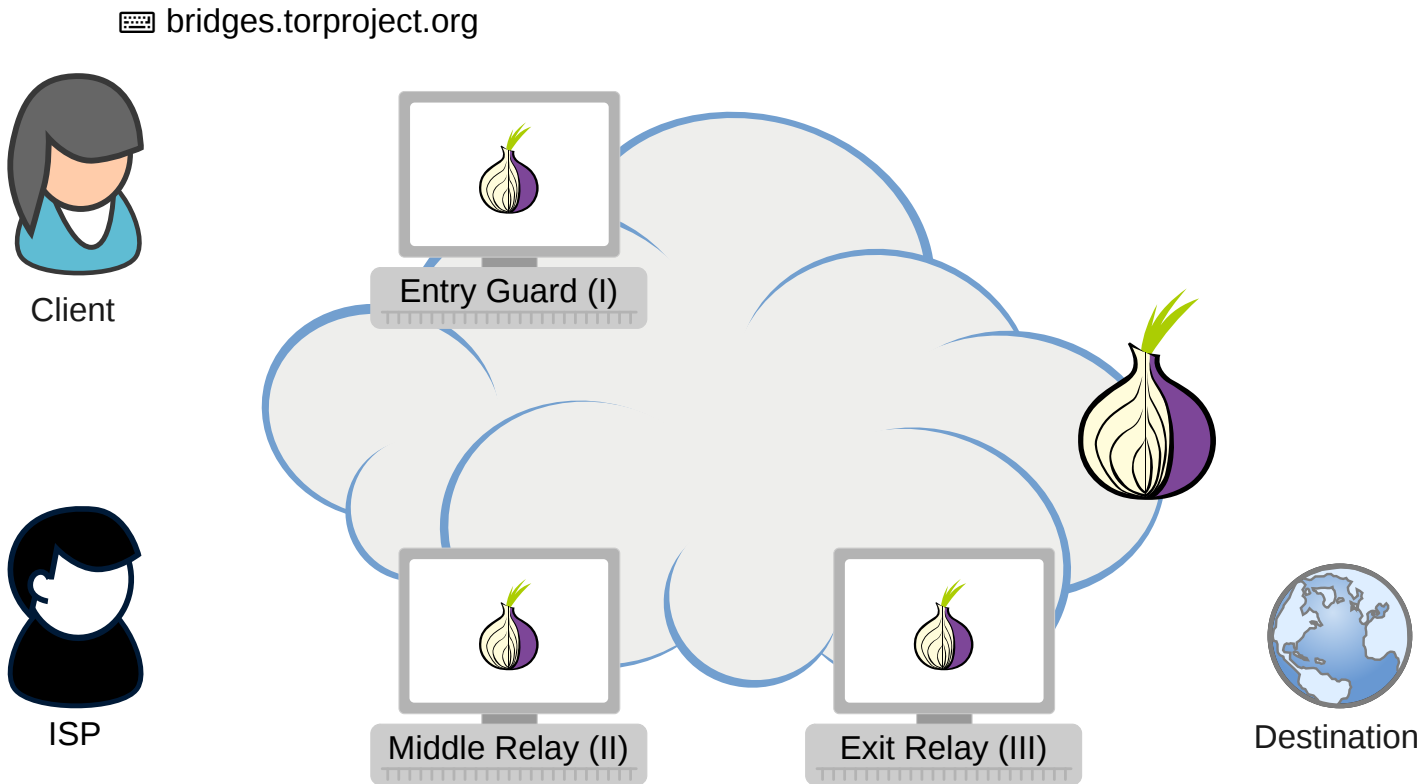
Tor Bridges

- If using Tor is
  - blocked by censorship
  - dangerous or considered supicious
- Then you need to use a *bridge*
  - an alternative entry point to the network
  - makes it harder for your ISP to know that you are using Tor
- Get *bridges* from `https://bridges.torproject.org`

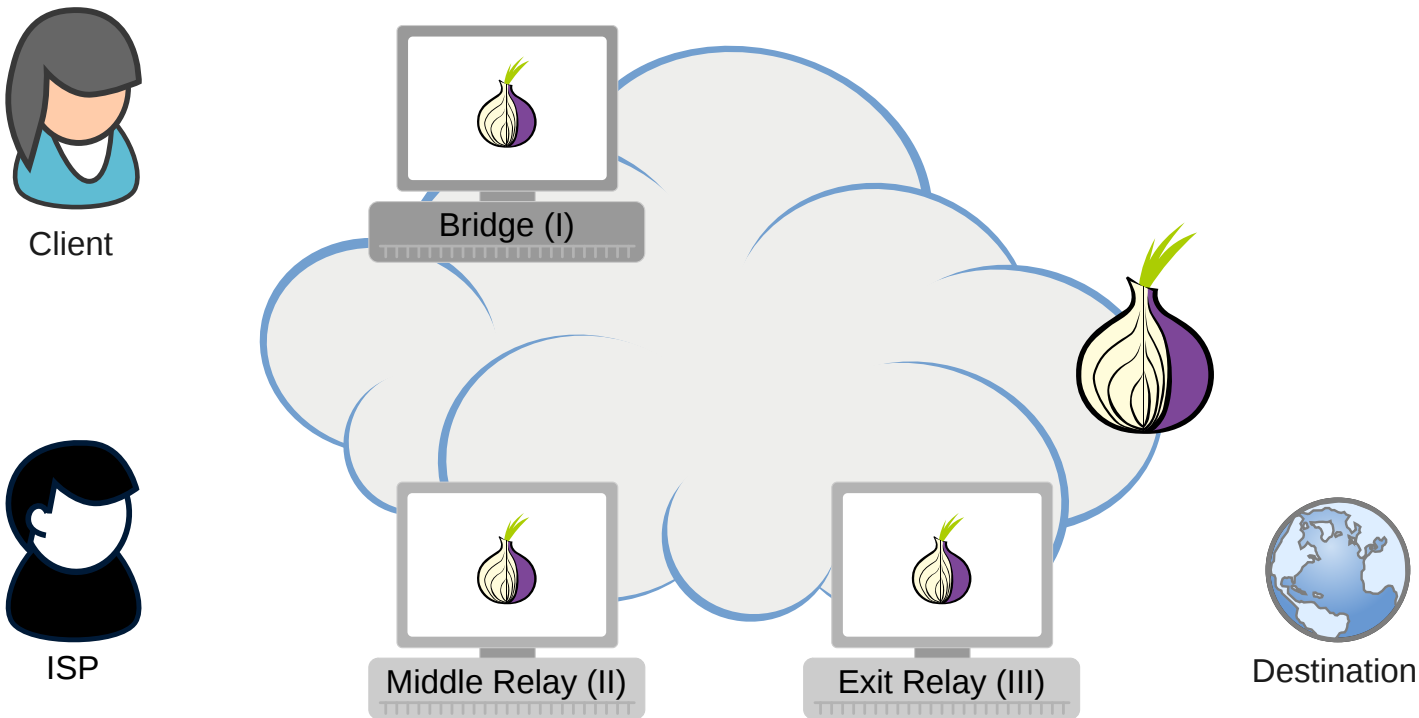
Using Tor Bridges



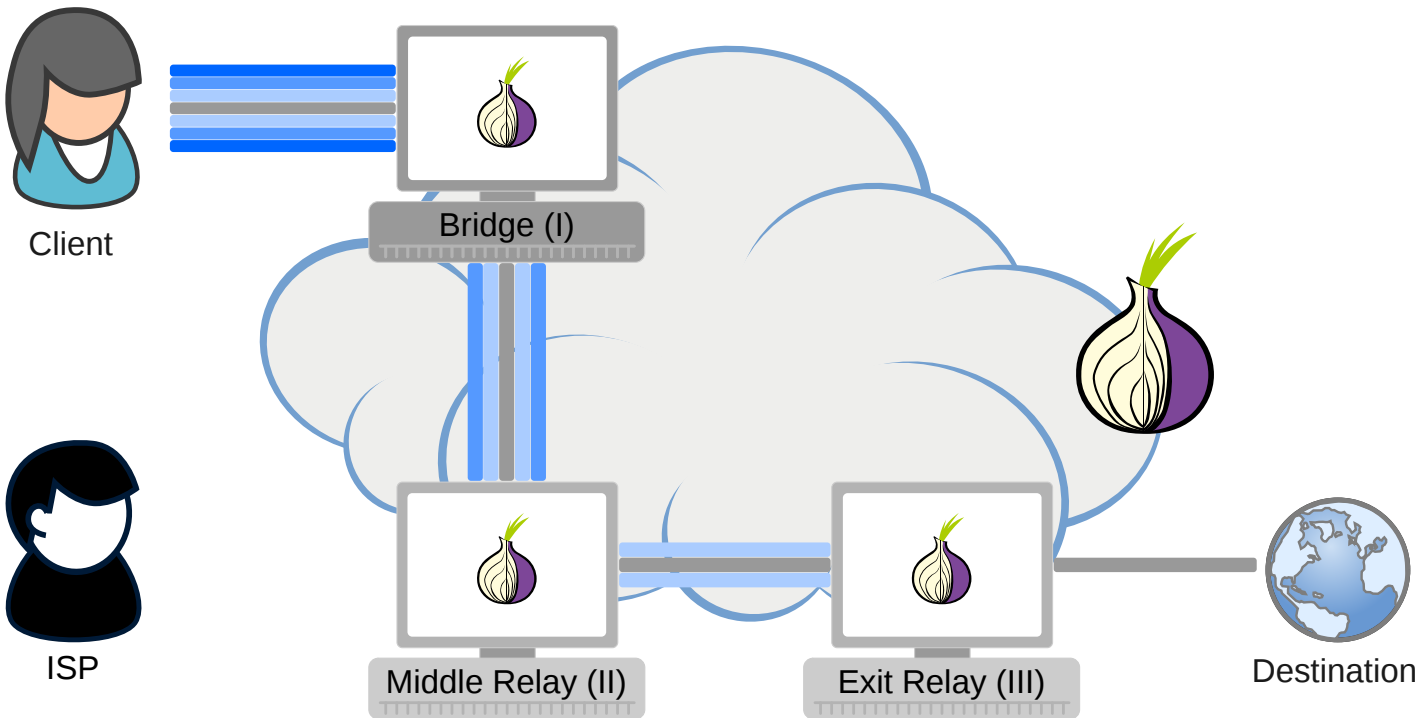
Using Tor Bridges



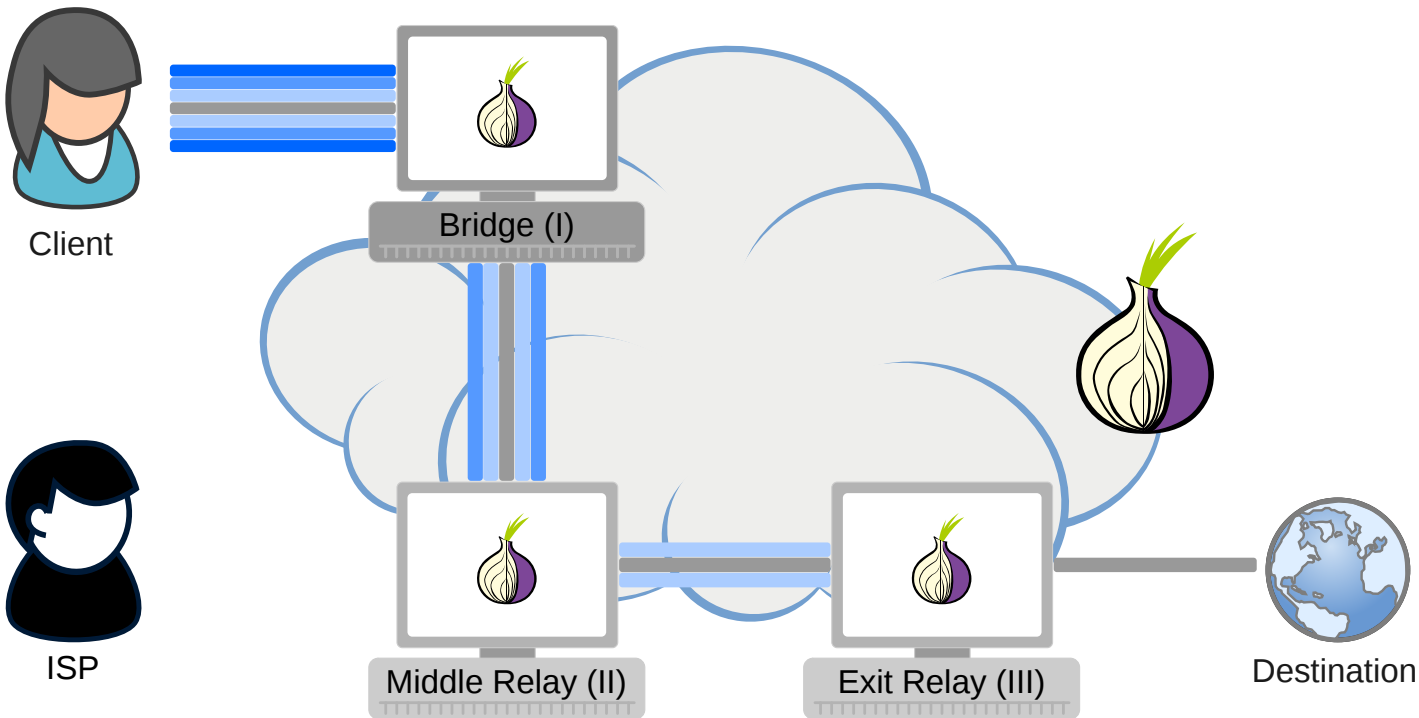
Using Tor Bridges



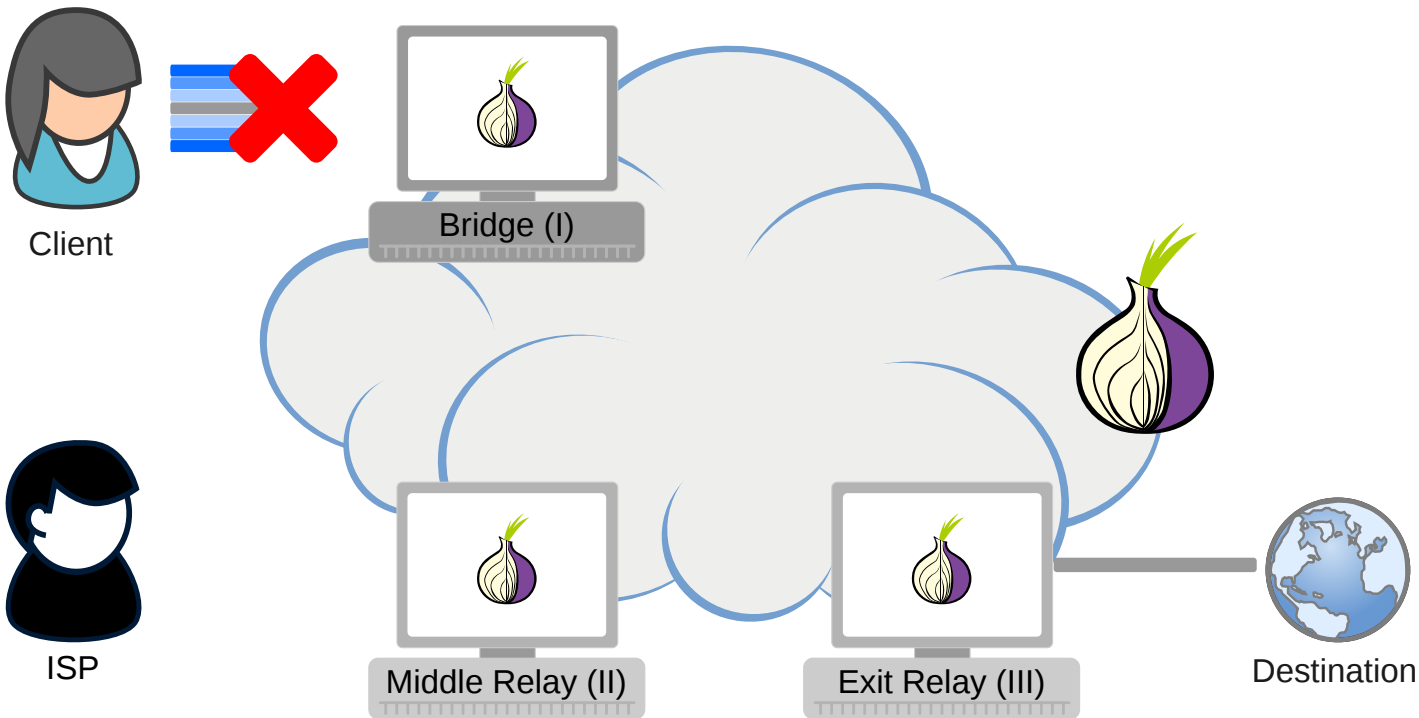
Using Tor Bridges



How Governments Censor Tor: Part II



How Governments Censor Tor: Part II



Pluggable Transports (PT)

- Censors can use DPI to recognize and filter Tor traffic

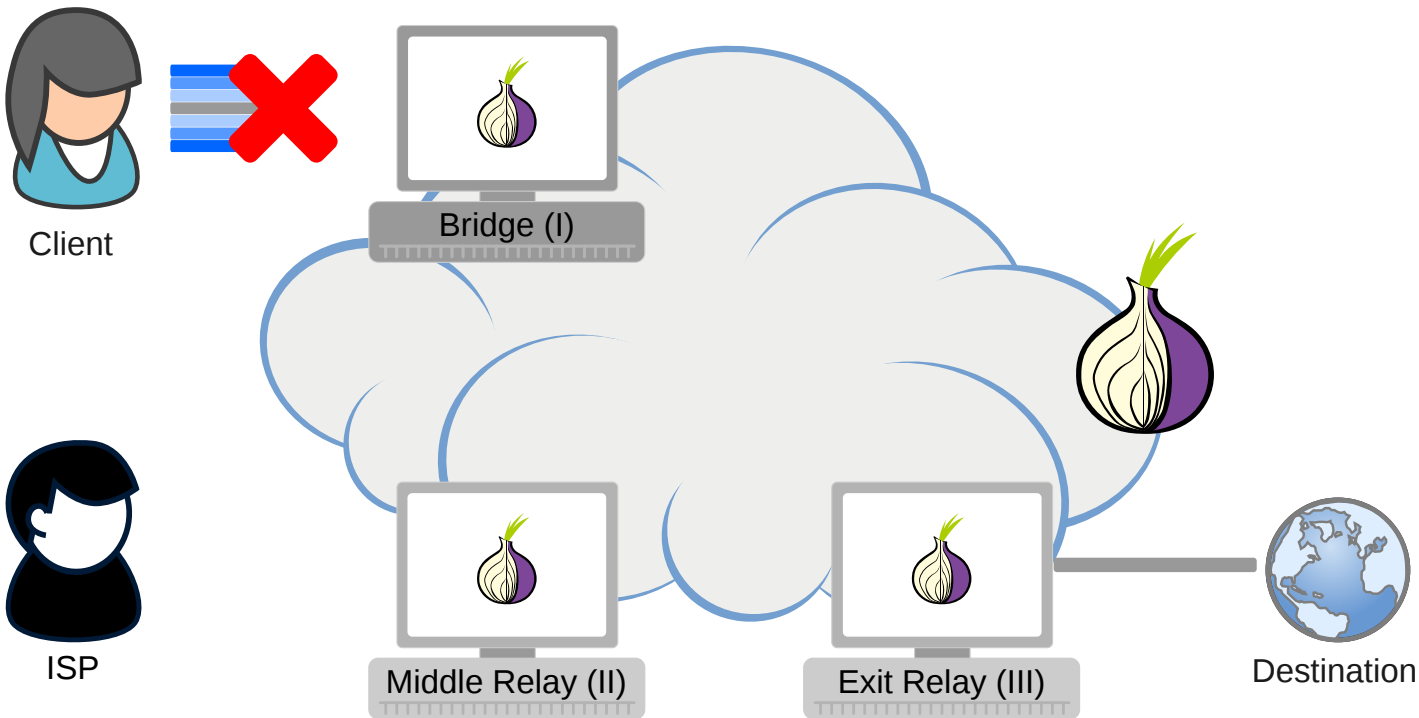
Pluggable Transports (PT)

- Censors can use DPI to recognize and filter Tor traffic
- *PT* transforms Tor traffic between client and the bridge
  - censors see innocent-looking traffic instead of Tor

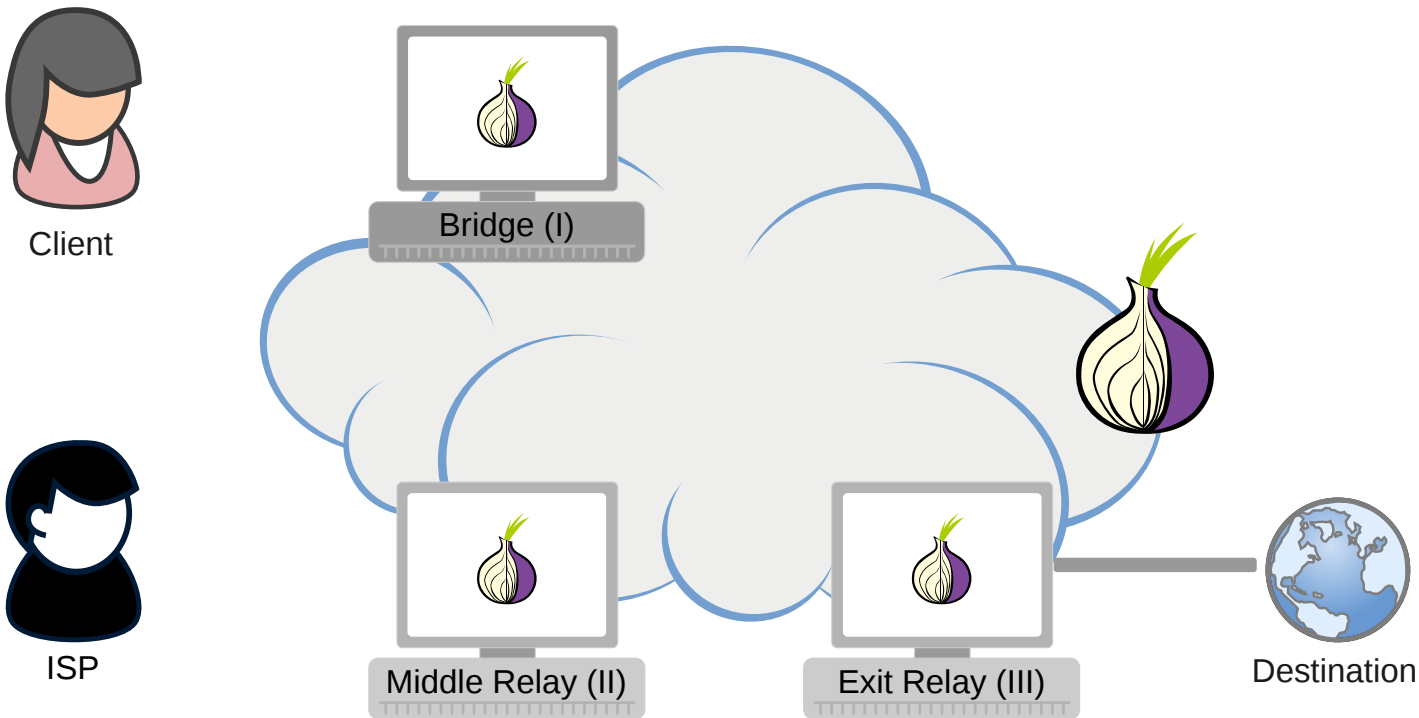
Pluggable Transports (PT)

- Censors can use DPI to recognize and filter Tor traffic
- *PT* transforms Tor traffic between client and the bridge
  - censors see innocent-looking traffic instead of Tor
- Use a *bridge* with a *PT* (obfuscated bridge)

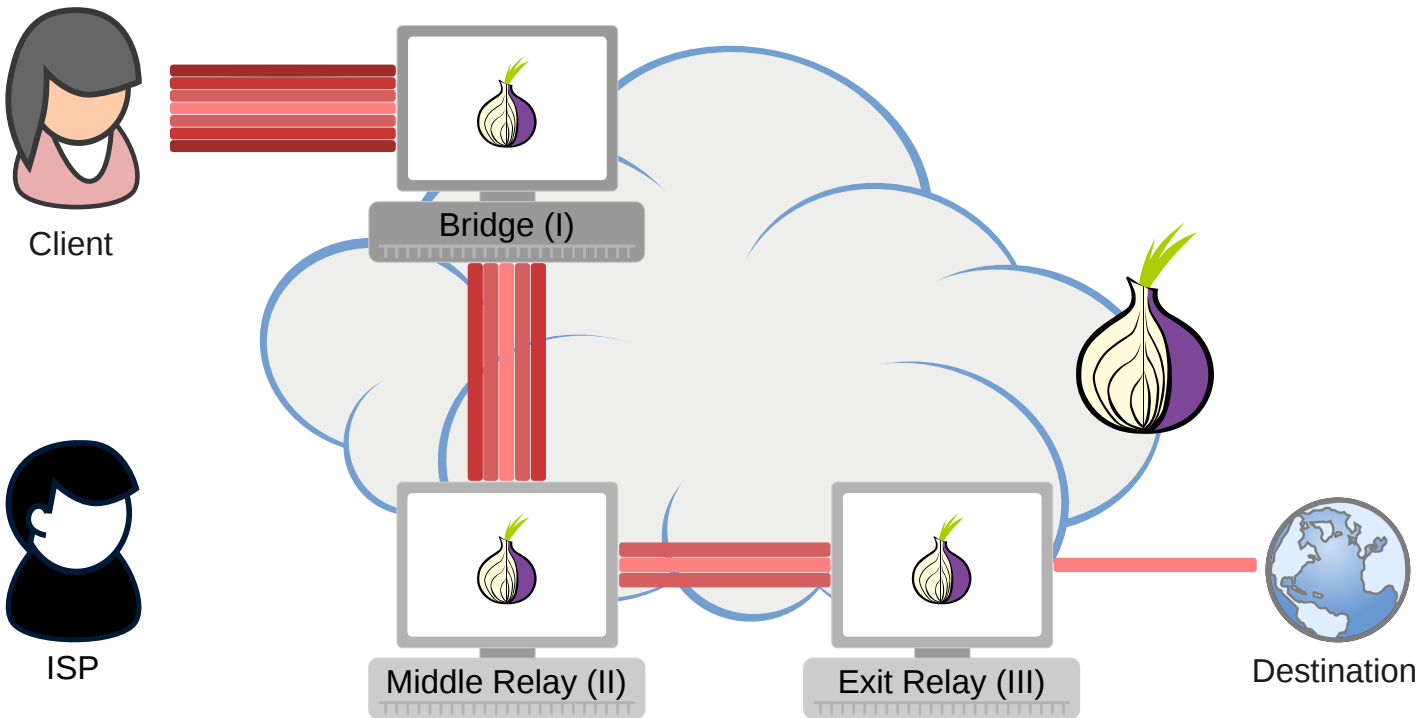
Using Pluggable Transports and Bridges



Using Pluggable Transports and Bridges



Using Pluggable Transports and Bridges

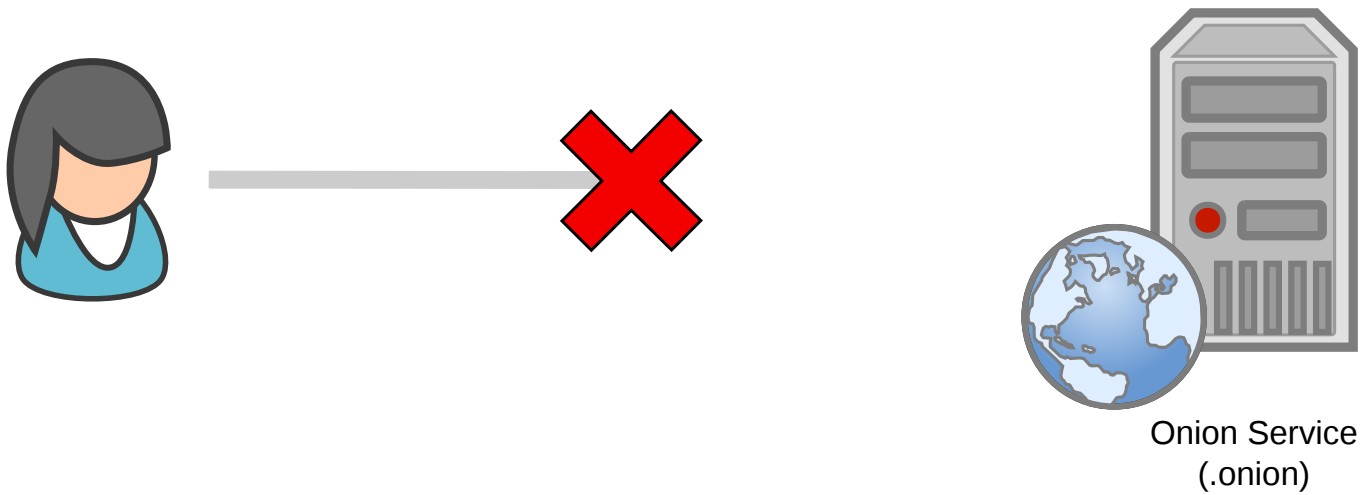


Bridges and Pluggable Transports: Demo

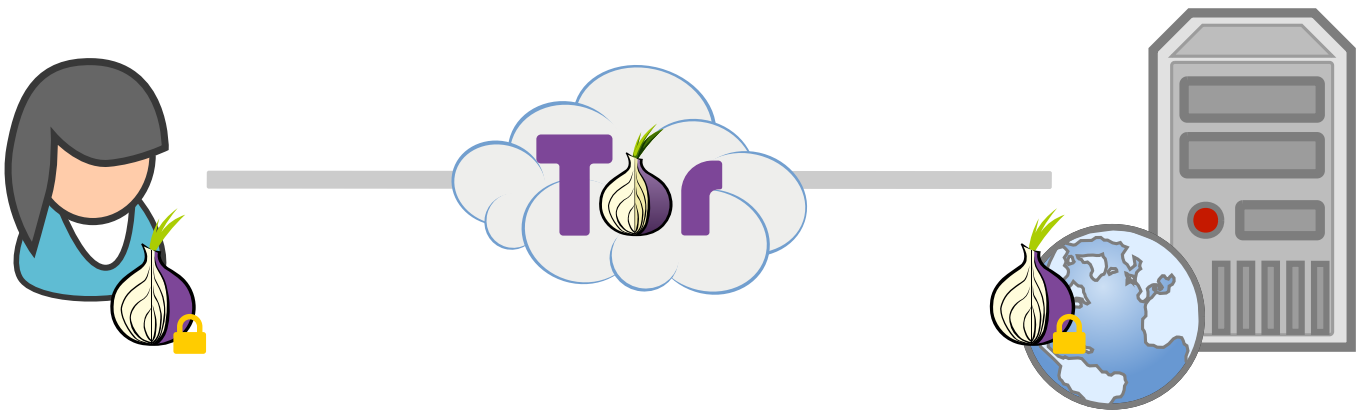
Using Tor Browser

Onion Services

Onion Services



Onion Services



Benefits of Onion Services

Benefits of Onion Services

- End-to-end encrypted without the need for a centralized CA

Benefits of Onion Services

- End-to-end encrypted without the need for a centralized CA
- Clients can be assured they are talking to the right address

Benefits of Onion Services

- End-to-end encrypted without the need for a centralized CA
- Clients can be assured they are talking to the right address
- The location and IP address of the onion service are hidden
  - making them difficult block or censor

Onion Services: Demo

The New York Times *Onion Service*:

`nytimes3xbfgragh.onion`

Tor vs. VPN

†	VPN	Tor	Tor Browser

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++
Appear Elsewhere	++	+	+

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++
Appear Elsewhere	++	+	+
Anonymity	+	++	+++

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++
Appear Elsewhere	++	+	+
Anonymity	+	++	+++
Privacy	–	+	+++

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++
Appear Elsewhere	++	+	+
Anonymity	+	++	+++
Privacy	−	+	+++
Speed	++	−−	−−

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Tor vs. VPN

†	VPN	Tor	Tor Browser
Censorship Evasion	++	+++	+++
Appear Elsewhere	++	+	+
Anonymity	+	++	+++
Privacy	−	+	+++
Speed	++	−−	−−
Cost	−−	+++	+++

† Modified under CC BY-SA 4.0. Original work by Tim Sammut from https://teamsammut.com/blog/2015/08/tor-vs-vpn-and-proxies-slides.html

Secure Web Browsing: Discussion

EFF Surveillance Self-Defense

https://ssd.eff.org

Thank You

Questions?

https://www.torproject.org/support/

sukhbir@torproject.org

E4AC D397 5427 A5BA 8450 A1BE B01C 8B00 6DA7 7FAA