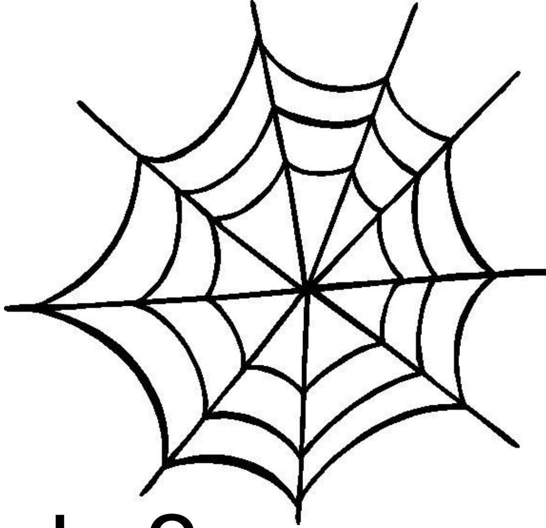
Anonymous Networks

Bradley Booth, Eric Dao, Aly Wakif



Why Anonymous Networks?

Ideally Used for the Principles of FOSS (Free and open-source Software):

“Free software” means software that respects users' freedom and community. Roughly, it means that the users have the freedom to run, copy, distribute, study, change and improve the software… Think free as in ‘free speech’ not as in ‘free beer’.” - GNU Philosophy

Services provided by anonymous networks:

Users can access the Internet while blocking any tracking or tracing of their identity on the Internet.

Prevent/make it more difficult traffic to perform analysis and network surveillance.

Access to functionality such as chat, email, forums where CIA is preserved.

Access to hidden websites.

P2P anonymous file sharing.

Services and Ownership are Split up Between Multiple Programs

I2P is an anonymous overlay network - a network within a network.

Intended to protect communication from surveillance and monitoring by third parties such as ISPs.

When to use:

Anonymous email service

Real time chat (instant messaging and IRC chat)

Blogging

P2P File sharing (Bittorrent)

Many more..

FREENET

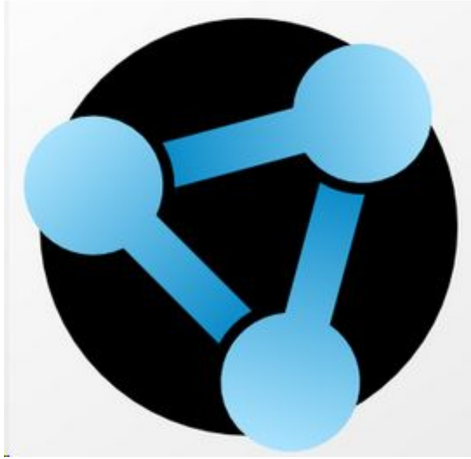
> I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say Daddy, where were you when they took freedom of the press away from the Internet.
>
> - Mike Godwin, Electronic Frontier Foundation

When to use:

Anonymously share files

Browse and publish "freesites" (web sites accessible only through Freenet)

Chat on forums, without fear of censorship.



A decentralized, private and secure communication and sharing platform.

Establish encrypted connections to create a network of computers, and provides various services.

Designed to provide maximum security and anonymity to its users beyond direct friends.

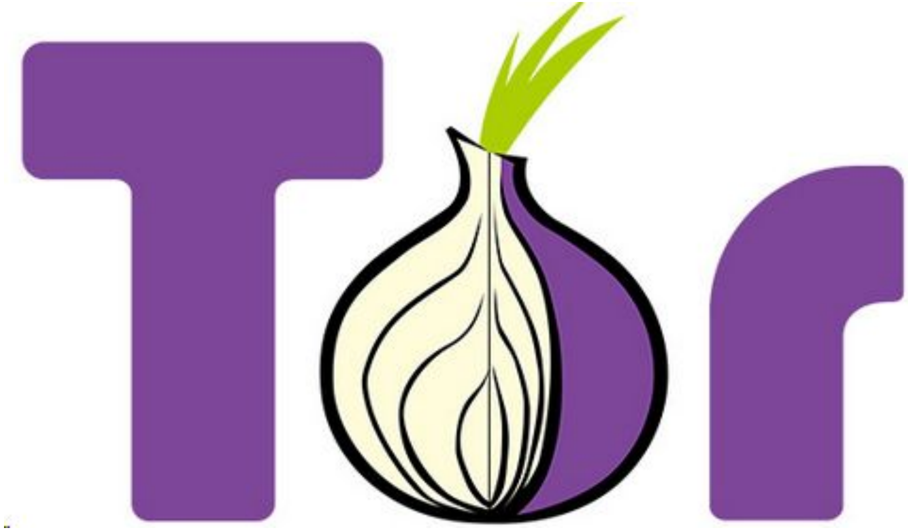
When to use:

Chat

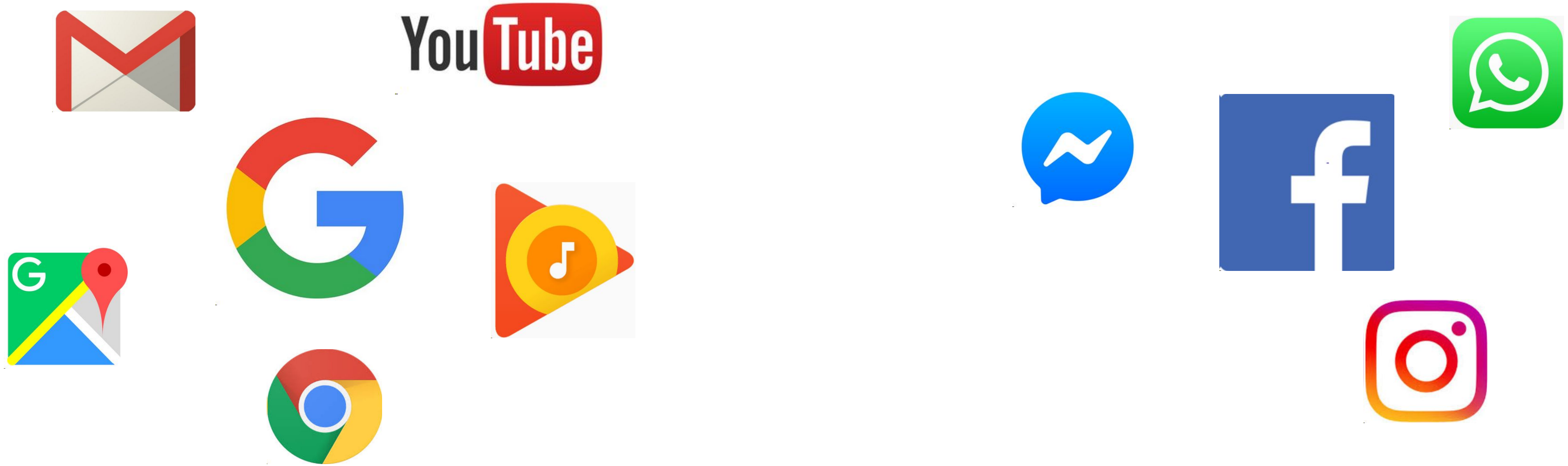
Forum

Mail

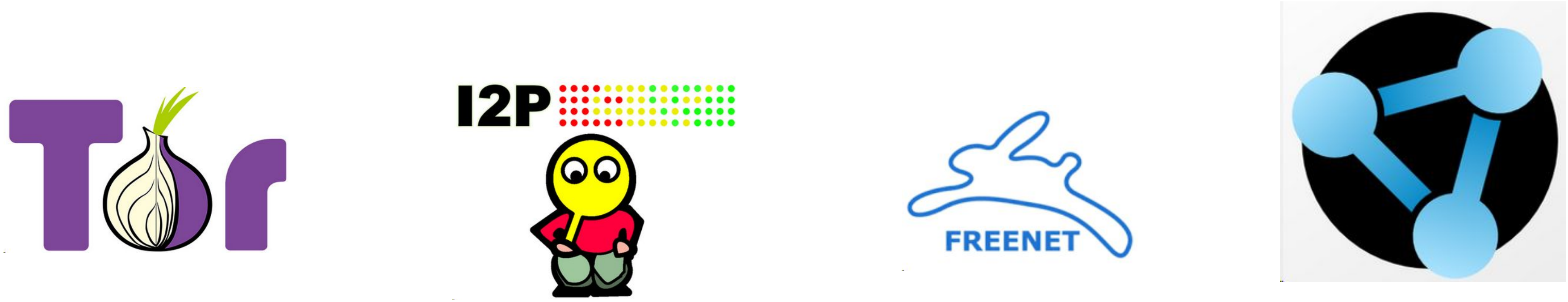
File sharing



A main focus of this presentation, so I won’t talk about it here.



Differences between the two sides?

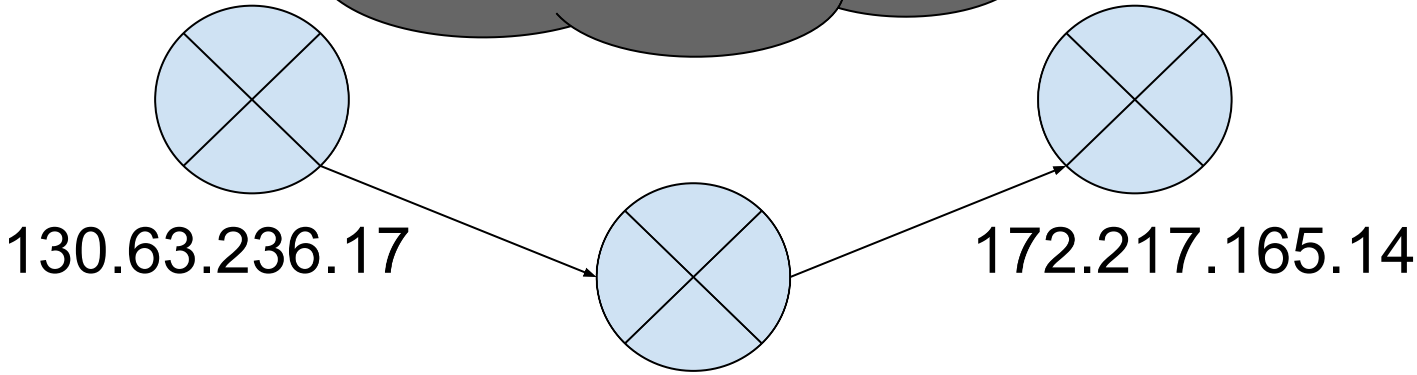


How Do They Work?
(Tor)

How does Tor work?

- T.O.R.: The Onion Router - Has layers on layers to hide the user behind
- Tor browser used to access Tor network, helps create a “Tor IP”
- Every machine benefitting from Tor joins the network as a node
- Nodes are also “routers” for the network - Tor calls some of these relays
- Router knows of A and B, forwards packets from A to B and from B to A
- Does not know who A or B connect to
- Everything sent between two nodes is encrypted at the application layer
- The paths are randomly generated

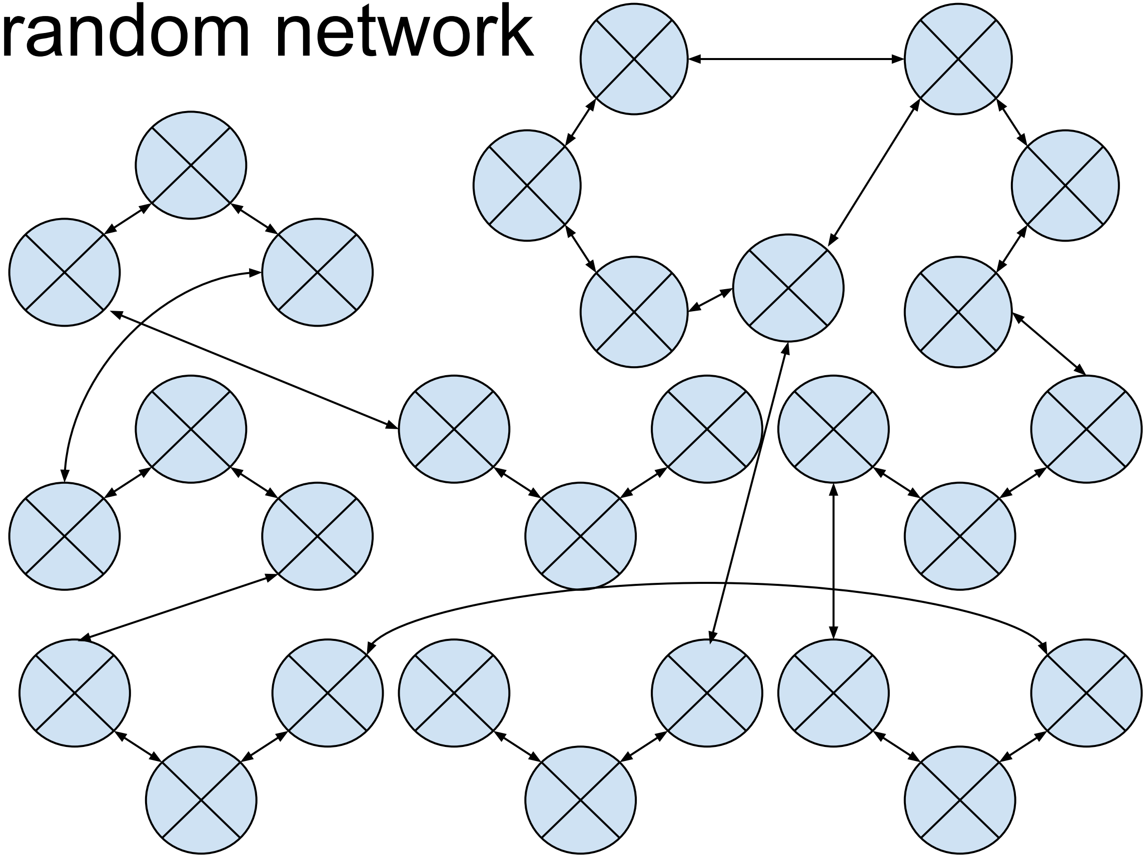
Don’t Know How The Rest Looks



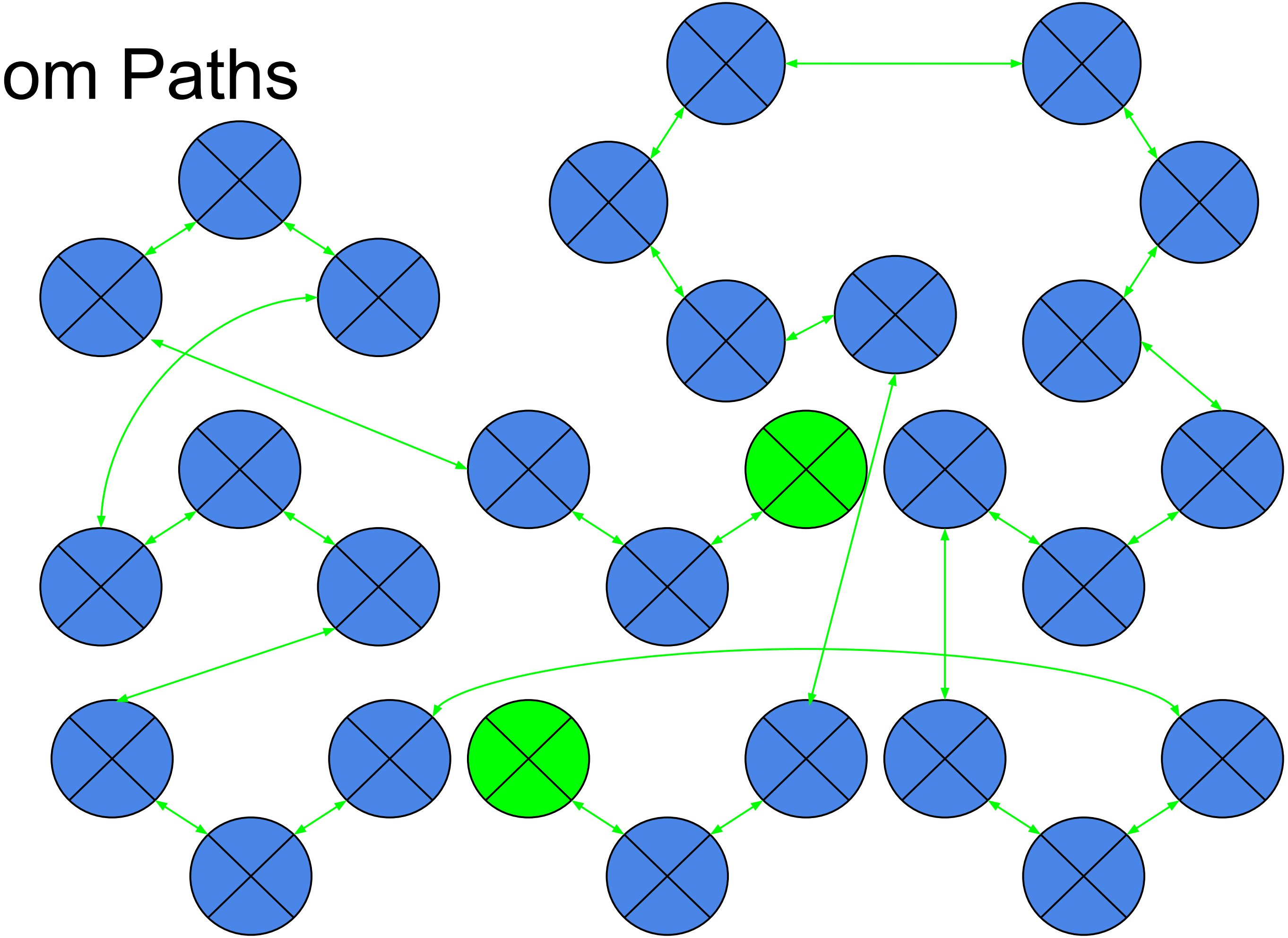
I am 151.101.1.67

I know:
130.63.236.17
172.217.165.14

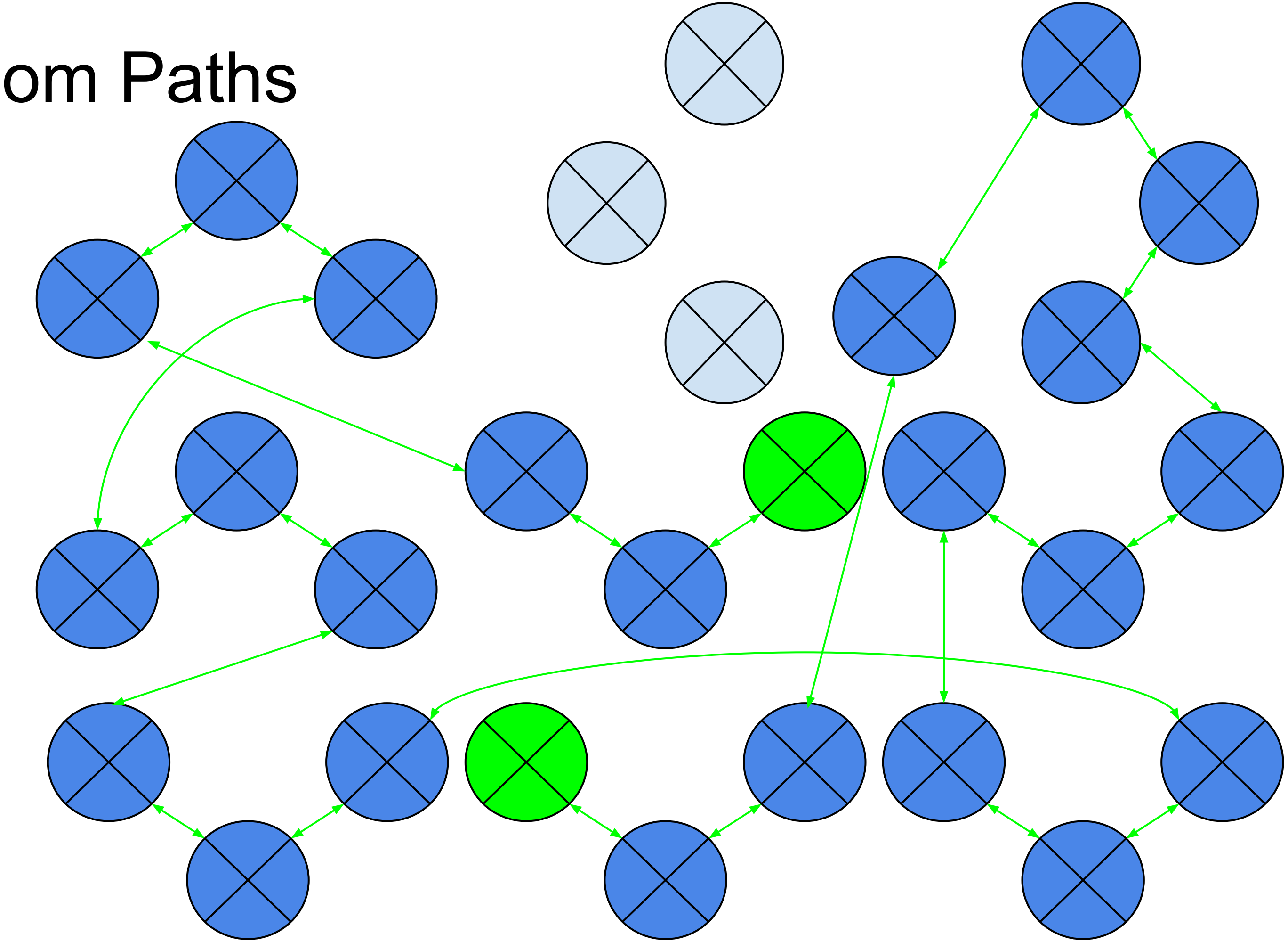
A huge, random network



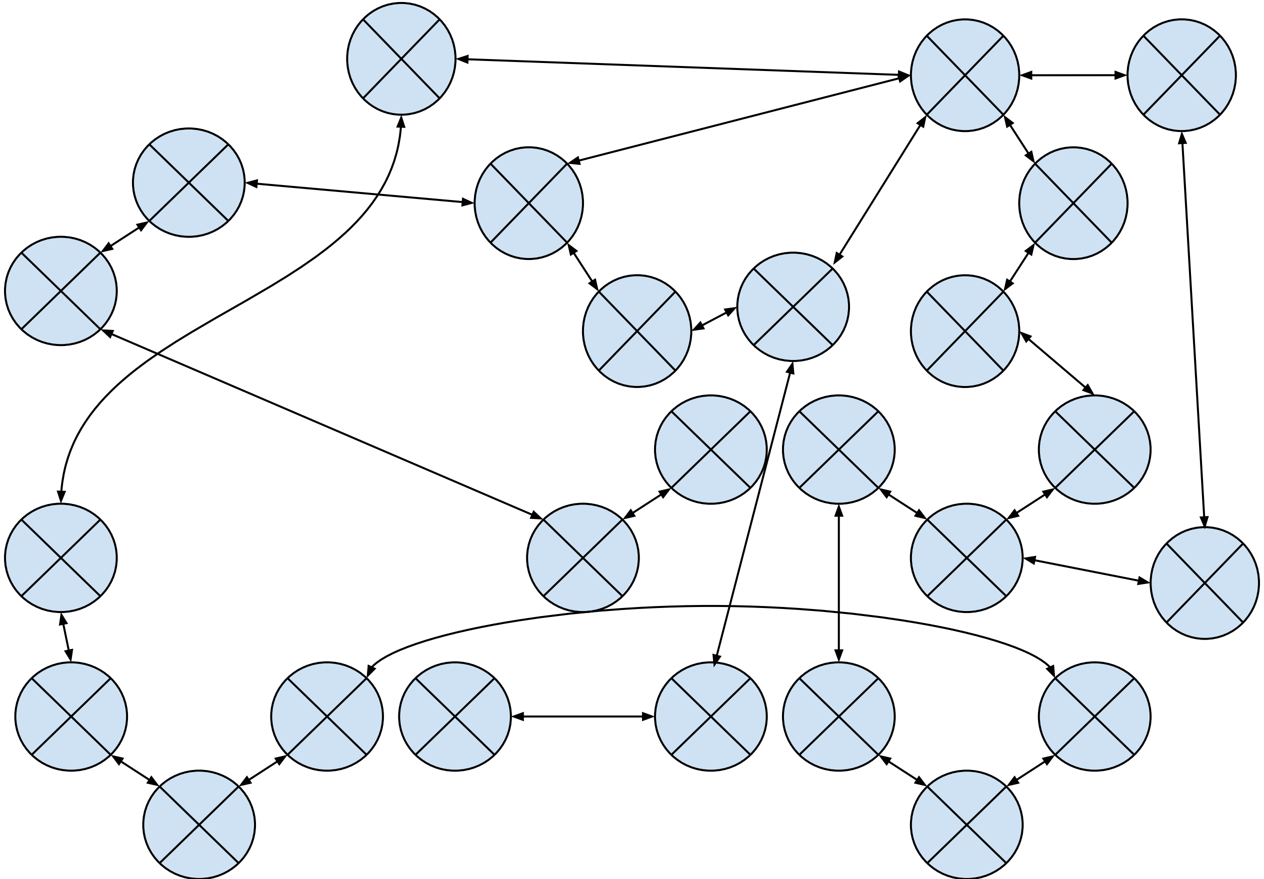
Random Paths



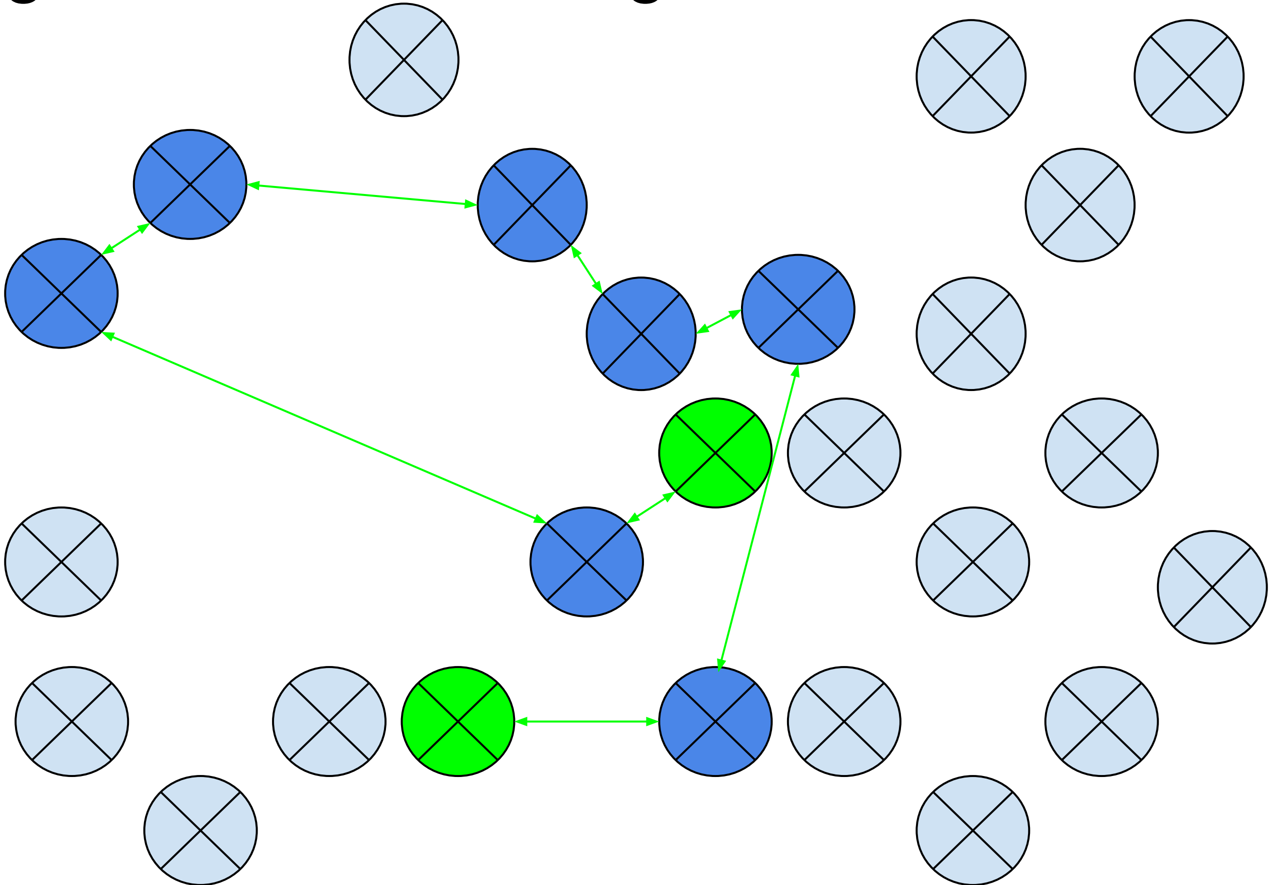
Random Paths



Network Constantly Changes



Meaning New Paths Emerge



Perfect Anonymity: Good and Bad

The Good

- Tor was initially meant to protect intelligence communications (DARPA+USNRL)
- Used by journalists and whistleblowers
- Used during various movements such as the Arab Spring
- Used by civilians in countries with limits, surveillance or censorship to speak
- Avoids online tracking
- Still used by military and law enforcement

The Bad

- Plaintext is still plaintext
- Used for criminal activity (Silk Road, hitmen)
- Makes criminals anonymous
- Any node could sniff traffic
- Tor users are subject to suspicion
- Access to the Dark Web - majority of these sites are actually .onion
- You may face legal action (exit nodes)
- Really slow
- Uses large amounts of bandwidth (512B per IRC line)

Tor’s Response:

“Criminals can already do bad things. Since they're willing to break laws, they already have lots of options available that provide better privacy than Tor provides. They can steal cell phones, use them, and throw them in a ditch; they can crack into computers in Korea or Brazil and use them to launch abusive activities; they can use spyware, viruses, and other techniques to take control of literally millions of Windows machines around the world.

Tor aims to provide protection for ordinary people who want to follow the law. ***Only criminals have privacy right now, and we need to fix that****...*

...So yes, criminals can use Tor, but they already have better options, and it seems unlikely that taking Tor away from the world will stop them from doing their bad things. At the same time, Tor and other privacy measures can fight identity theft, physical crimes like stalking, and so on.” -TorProject Abuse FAQ

Former Executive Director Andrew Lewman

“What’s changed most about Tor is the drug markets have taken over,” Lewman said. “We had all these hopeful things in the beginning but ever since Silk Road has proven you can do it, the criminal use of Tor has become overwhelming. I think 95 percent of what we see on the onion sites and other dark net sites is just criminal activity. It varies in severity from copyright piracy to drug markets to horrendous trafficking of humans and exploitation of women and children.”

-May 22, 2017: https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/

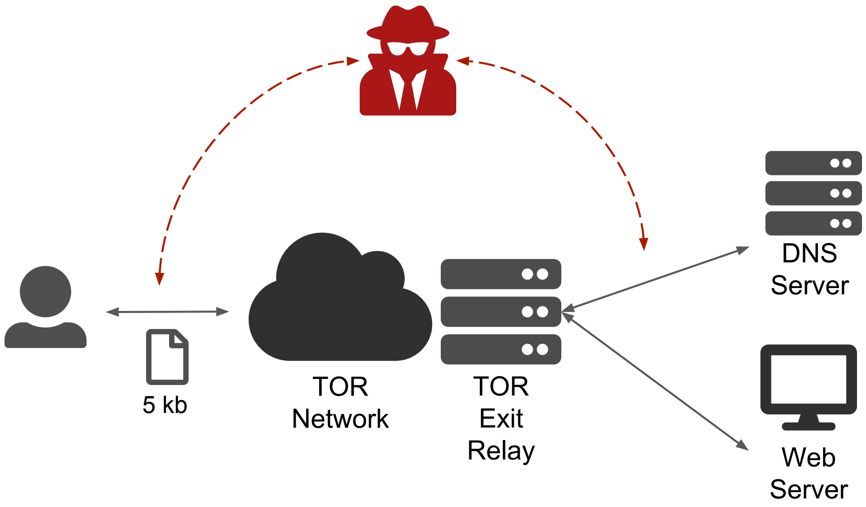
Onion Routing Gets Stronger With More Users!

You may be helping the good guys or the bad guys by acting as a relay. That’s scary. That’s anonymity.

Vulnerabilities

DefecTor Correlation Attack

Goal: Deanonymize victim

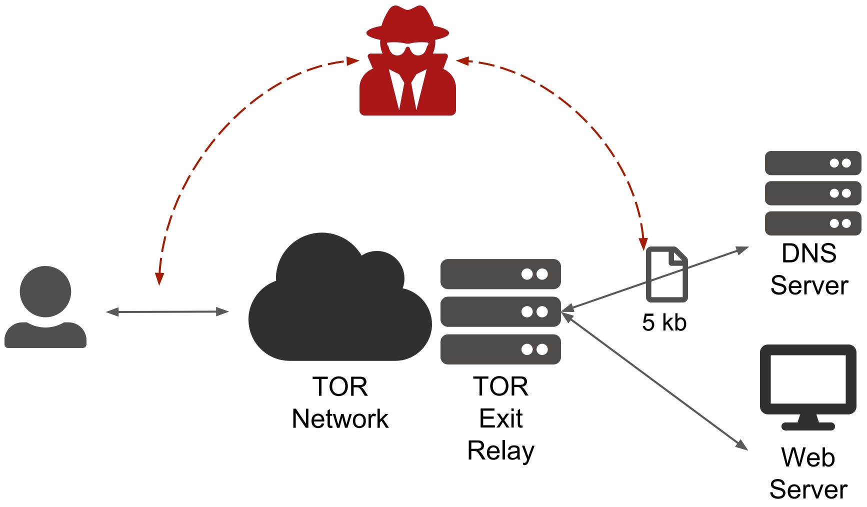


User sends 5kb request at 10:00:00

https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
https://www.helpnetsecurity.com/2016/09/30/defector-attacks-against-tor-users/

DefecTor Correlation Attack

Goal: Deanonymize victim

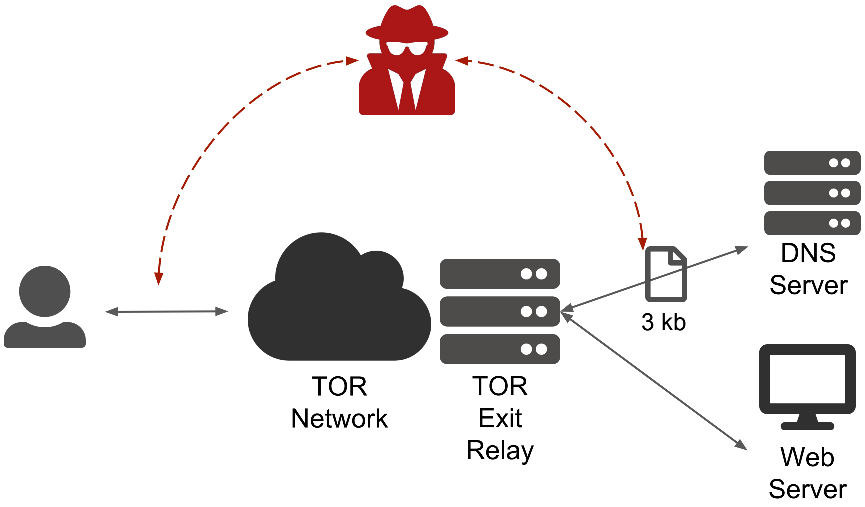


5kb request is seen at 10:00:01

https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
https://www.helpnetsecurity.com/2016/09/30/defector-attacks-against-tor-users/

DefecTor Correlation Attack

Goal: Deanonymize victim

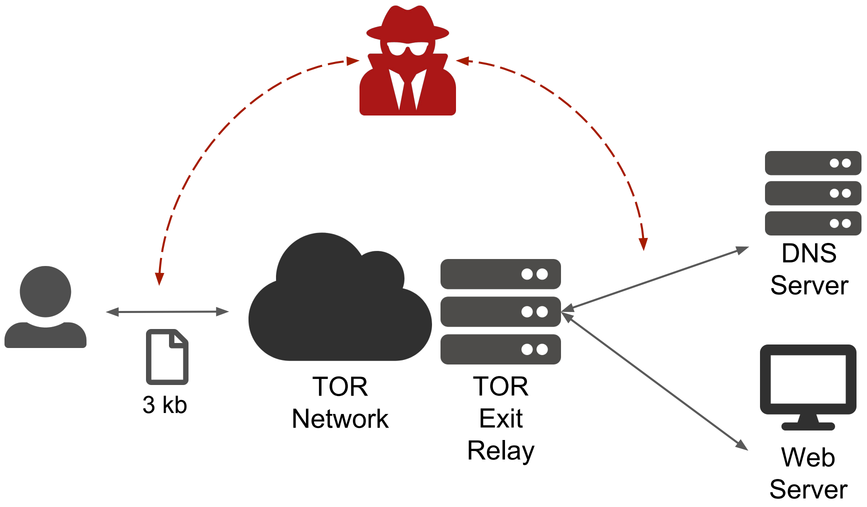


3 kb request is seen at 10:00:01

https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
https://www.helpnetsecurity.com/2016/09/30/defector-attacks-against-tor-users/

DefecTor Correlation Attack

Goal: Deanonymize victim

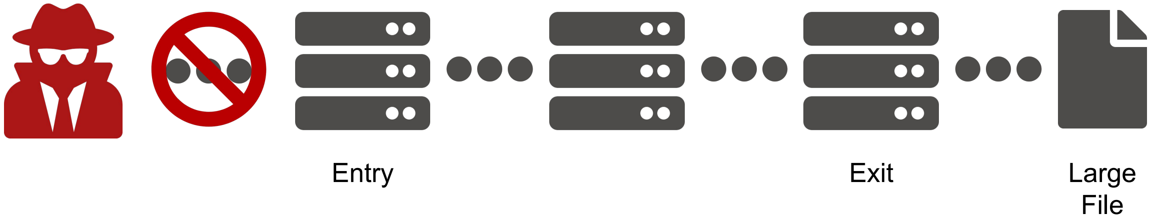


3 kb request is received at 10:00:02

https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
https://www.helpnetsecurity.com/2016/09/30/defector-attacks-against-tor-users/

TOR “Sniper Attack” DoS

Goal: Exploit flow algorithm to deplete victim memory resources



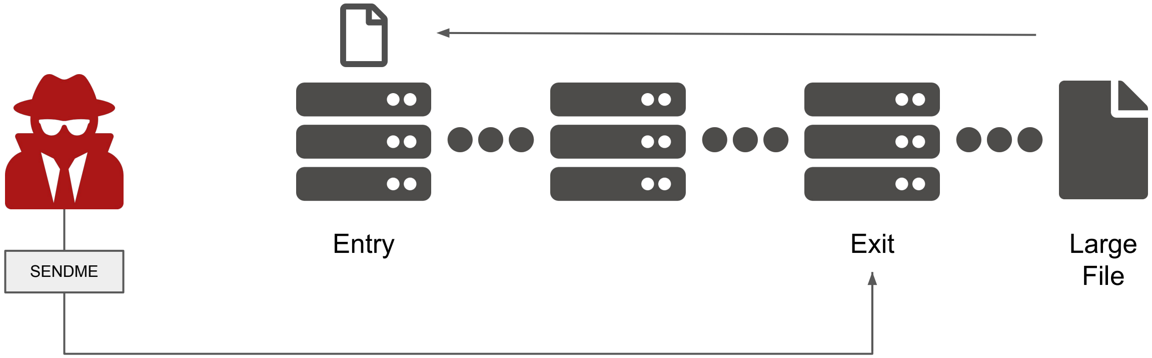
Adversary then ignores the TCP connection to entry relay

Adversary initiates large download request

https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses

TOR “Sniper Attack” DoS

Goal: Exploit flow algorithm to deplete victim memory resources



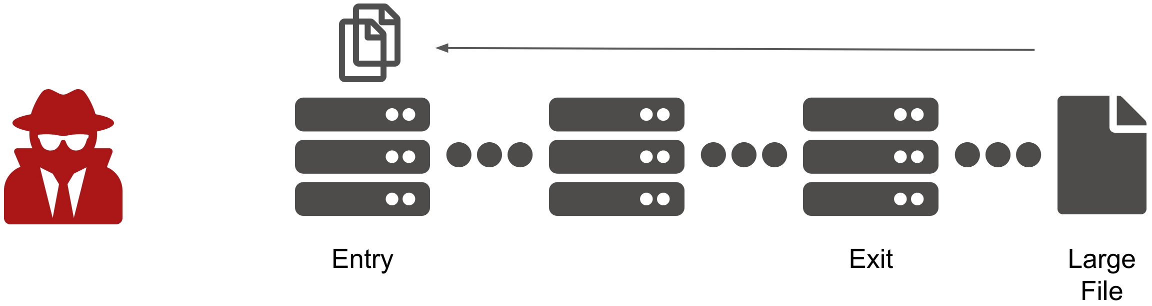
User sends a “SENDME” request imitating the entry relay to the exit relay

Data is sent from external server back over circuit

https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses

TOR “Sniper Attack” DoS

Goal: Exploit flow algorithm to deplete victim memory resources

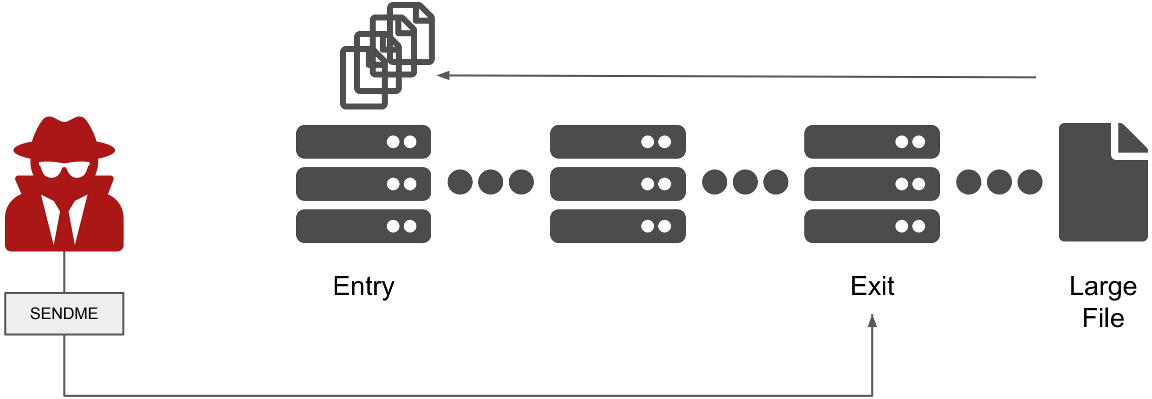


This causes the exit relay to send more data along the circuit

https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses

TOR “Sniper Attack” DoS

Goal: Exploit flow algorithm to deplete victim memory resources

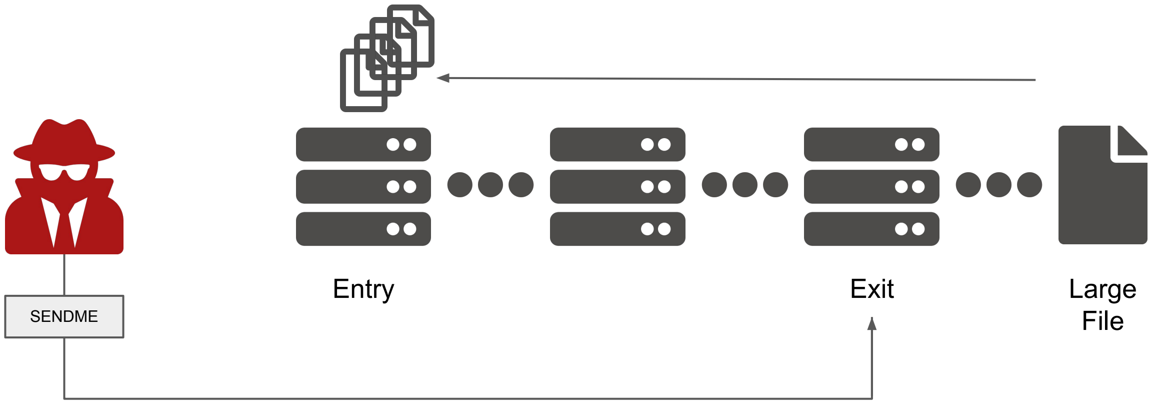


This process is repeated until the memory of the entry relay is used up

https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses

TOR “Sniper Attack” DoS

Goal: Exploit flow algorithm to deplete victim memory resources

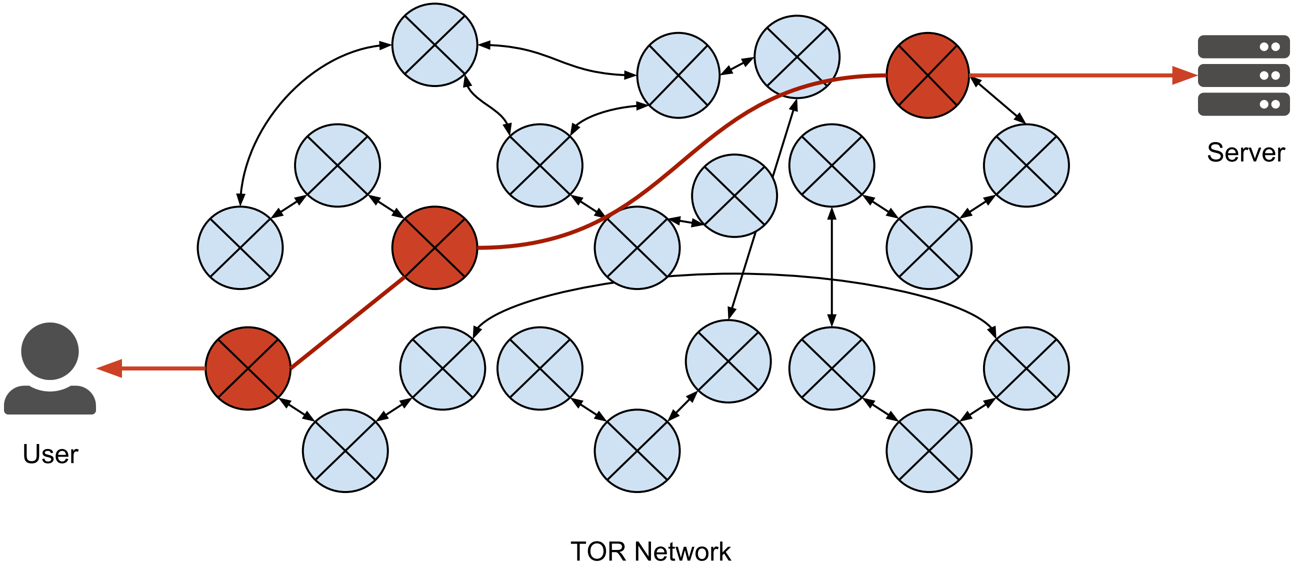


This is effective when multiple requests are executed in parallel

https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses

TOR Debian OpenSSL Exploit

Goal: Exploit weak cryptography vulnerability to deanonymize a user



https://blog.torproject.org/debian-openssl-flaw-what-does-it-mean-tor-clients

References

[1]. https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack
[2]. https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses
[3]. https://blog.torproject.org/debian-openssl-flaw-what-does-it-mean-tor-clients
[4]. https://www.gnu.org/gnu/gnu-history.html
[5]. www.stallman.org/
[6]. https://www.pinterest.ca/pin/600456562790868553/
[7]. https://www.helpnetsecurity.com/2016/09/30/defector-attacks-against-tor-users/
[8]. https://geti2p.net/en/
[9]. https://www.techopedia.com/definition/25187/anonymity-network
[10]. https://freenetproject.org/author/freenet-project-inc.html
[11]. https://retroshare.cc/