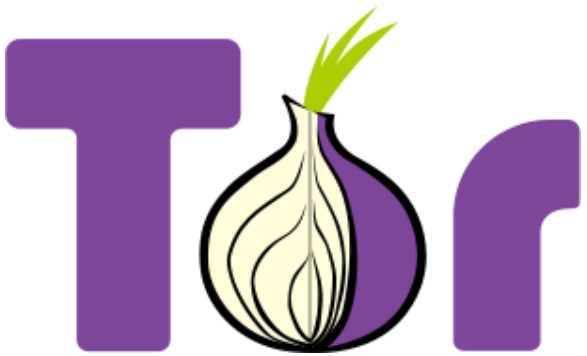
Intro to Tor 

UC Davis Cybersecurity Club
Nate Buttke

February 3, 2022

What is Tor?

- Tor: The onion router
- Why "onion?" Encrypted in layers...
- 1990s: U.S. Navy creates onion routing.
- 2002: Tor was developed under a contract for the United States Naval Research Laboratory
- 2006: Original authors release Tor as free software (BSD license), and Tor Project 501(c)(3) is formed.
- Tor still receives most of its funding from the U.S. government and military. Some see this as a liability.



Onion routing

There are layers of encryption: each relay removes one layer of encryption. If you are browsing the clearnet through Tor, your exit node decrypts the final layer before passing your request to its internet destination.

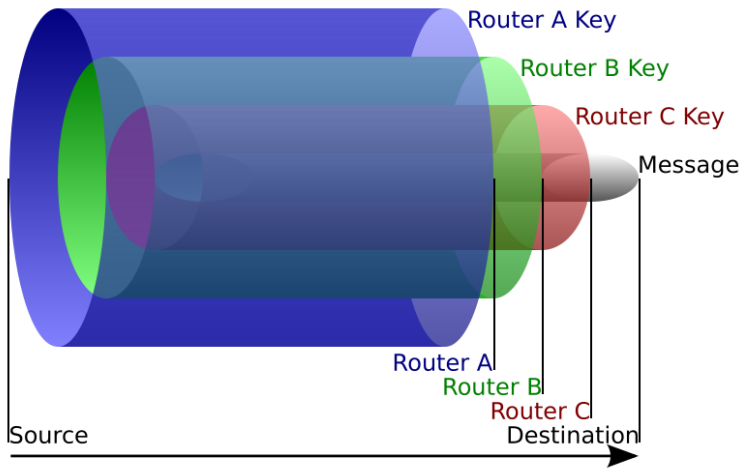
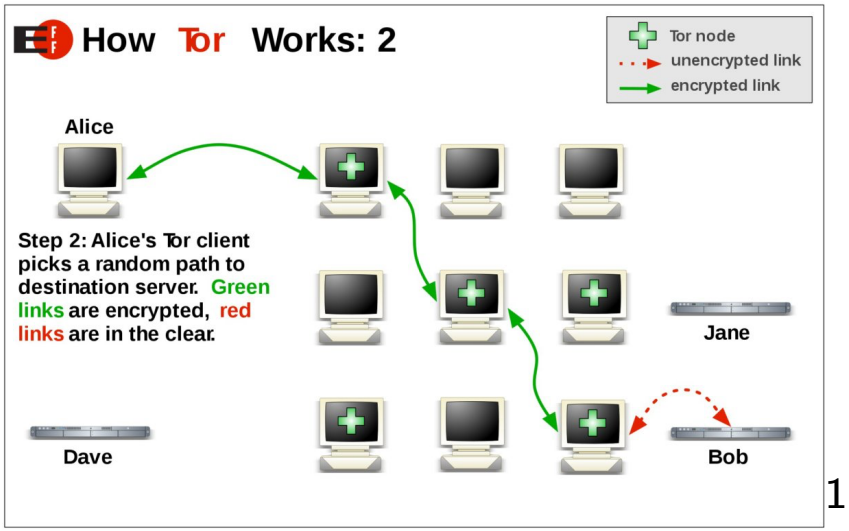
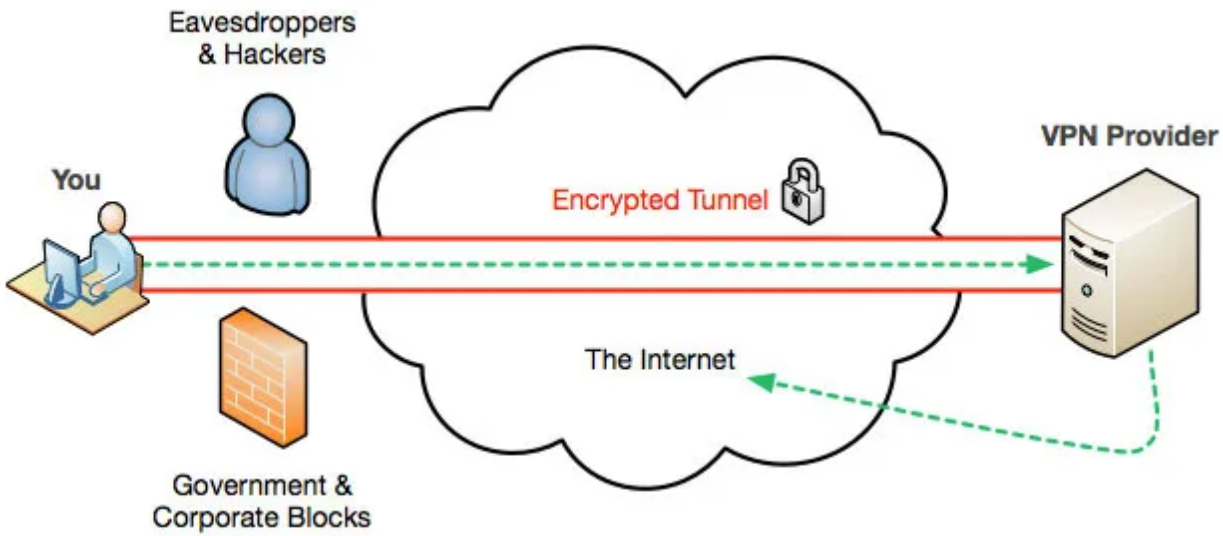


Figure: Onion Routing
English Wikipedia user HANtwister, CC BY-SA 3.0, via Wikimedia Commons

Tor vs. VPNs



[1]



[1] (also: doesn't *have* to exit the Tor network)

The Tor Browser Bundle

History: Tor used to be distributed as just a proxy. You would bring your own web browser, and point it to `127.0.0.1:9050`. This is susceptible to fingerprinting and other vulnerabilities.

The Tor Browser Bundle was introduced for safety and anonymity (everyone's browser looks the same).

Anatomy of a .onion address

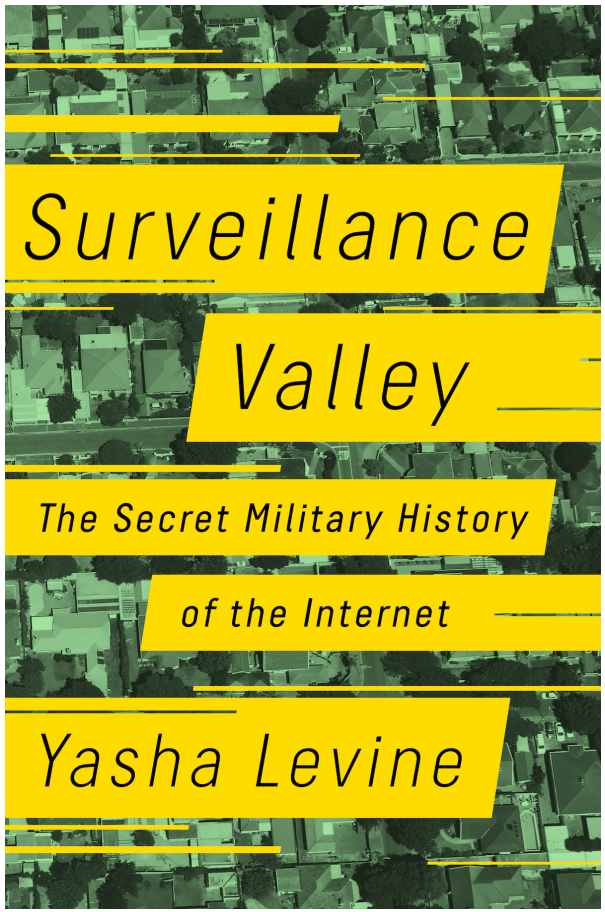
- v2 addresses, e.g. `facebookcorewwwi.onion`
  - deprecated in 2021: used RSA1024 and 80 bit SHA1 addresses
  - "the permanent identifier of the hidden service, consisting of 80 bits. It can be calculated by computing the hash value of the public hidden service key and truncating after the first 80 bits" [3].
- v3 addresses: 56 characters, e.g.

  `nategbee2zejhurhw3fbhbc5pzgu2hzerydy7ajs2tclnbxhwoc6icqd.onion/`
  - ed25519: eliptic curve cryptography.
  - The address is a function of the public key.[2]
  - "A hidden service's name is its long term master identity key. This is encoded as a hostname by encoding the entire key in Base 32, including a version byte and a checksum, and then appending the string '.onion' at the end. The result is a 56-character domain name" [4].

[2] This is why we must "mine" for vanity addresses. Not dissimilar to hashcat.

Tor: a mathematical[3] solution to a political problem

- Tor provides a clever defense against government surveillance, even social graph or metadata analysis
- Cryptographic arms race against the state: censorship and surveillance techniques evolve alongside Tor [1].
- Should we need to send our traffic all over the world to communicate safely with our neighbors? Is this wasteful?



[2]

[3] i.e. cryptographic

Workshop

Any questions before hands-on demo?

How to browse onion services[4]

- In Kali, open Tor Browser.
- Install any updates.
- Connect to Tor.
- Visit clearnet or onion websites.
- The Phobos search engine indexes some onion services. I will include a link at `https://nategb.xyz/cybersec/tor`

[4] "onion service" is the new word for "hidden service"

How to ssh to an onion service[5]

What operating system is running on this host?

```
$ systemctl status tor       #(check Tor's proxy is available)
$ torsocks ssh \
cowsay@2svffbj7sslh7xbjrtvvr25clreikouznohbtblsttw6yjzripo77zqd.onion

$ sudo systemctl stop tor
```

[5] command may be copied from `https://nategb.xyz/cybersec/tor`

nginx configuration file

```
$ cat /etc/nginx/sites-available/cowsay.conf

server {
    listen localhost:80;
    listen unix:/var/run/cowsay.sock;

    server_name localhost;
    root /var/www/cowsay;
    index index.html;

    add_header Onion-Location http://PLACEHOLDER.onion$request_uri;

    location / {
        try_files $uri.html $uri $uri/ =404;
    }
}
^^I
```

create an index.html

```
$ sudo vim /var/www/cowsay/index.html

<!DOCTYPE HTML>
<html>

...
$ sudo ln -s /etc/nginx/sites-available/cowsay.conf /etc/nginx/sites-enabled/

$ sudo systemctl start nginx
$ curl localhost:80 || firefox localhost:80
your site here
$ curl --unix-socket /var/run/cowsay.sock localhost
your site here (via unix socket!)
```

If the Unix socket works, it's best to disable other listen directives.

Generate vanity address

- Recall that the .onion address is a function of the public key.
- On its own, Tor generates a keypair for the hidden services in `/etc/tor/torrc`.
- What if we just generate keypairs until the hostname is human-readable?
- Do you see the similarity to hashcat and password cracking?

mkp224o

mkp224o is a program to generate vanity addresses. It generates keypairs and addresses, compares the address to a wordlist, and throws out non-matches.
Make sure you have autoconf and libsodium-dev.

```
$ git clone https://github.com/cathugger/mkp224o.git
$ cd mkp224o
$ ./autogen.sh
$ ./configure  #(we are omitting optimization today)
$ make
$ name=cowsay #pick your own :)
$ ./mkp224o $name -B -d output_dir
```

The room's CPU fans blow

Install keys

```
$ sudo cp -r cowsay6v2s....onion /var/lib/tor/cowsay
$ sudo chown -R debian-tor: /var/lib/tor/cowsay
$ sudo chmod -R u+rwX,og-rwx /var/lib/tor/cowsay
```

Edit torrc

```
$ sudo vim /etc/tor/torrc

### This section is just for location-hidden services ###

HiddenServiceDir /var/lib/tor/cowsay
HiddenServicePort 80 unix:/var/run/cowsay.sock
# Unix socket is the best practice. Especially at school.

...

$ sudo systemctl start tor
```

Nice work

Congrats! You've got a website on the "dark web."

Works consulted, further reading:

[1] Roger Dingledine. "The Tor Censorship Arms Race The Next Chapter". In: 2019. URL: https://www.youtube.com/watch?v=ZB8ODpw_om8.

[2] Yasha Levine. *Surveillance Valley*. PublicAffairs, 2018. ISBN: 9781610399166.

[3] *Tor Rendezvous Specification - Version 2*. The Tor Project. URL: https://gitweb.torproject.org/torspec.git/tree/rend-spec-v2.txt.

[4] *Tor Rendezvous Specification - Version 3*. The Tor Project. URL: https://gitweb.torproject.org/torspec.git/tree/rend-spec-v3.txt.