Tor & Darknet Operations

BK 2024 - Special Topics

Background | Computer networking

If two computers want to communicate, they need to know each other's **IP addresses**, much like with real-world addresses for mail

If you're sending data over the internet, the machine receiving that data probably knows your IP

Background | How to think like a fed

Suppose you're a fed who wants to catch a cybercriminal. How do you track them down?

1. Take over a site they use and get their IP address from the logs (alternatively, have ISPs report any user who browses to that site)
2. Show up to an ISP with a warrant to get that IP address's owner
3. Raid their house

I'll create a GUI interface using Visual Basic
[to] see if I can track an IP address.

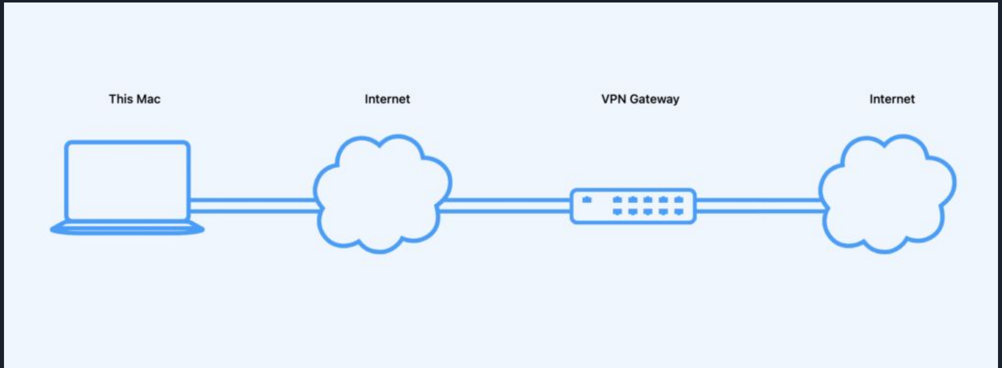
Background | How to think like a criminal

How do you prevent the feds from getting your IP if they can take over the websites you’re sending data to?

Background | How to think like a criminal

Idea 1: Use a VPN

- VPN = Virtual Private Network
- Your computer "tunnels" all of its traffic into a remote network, from where it can then be sent out to the open internet if necessary
- Any responses get forwarded back to you by the VPN
- **Websites see the VPN's IP instead of yours**



Fed time again

How would the feds catch someone who's behind a VPN?

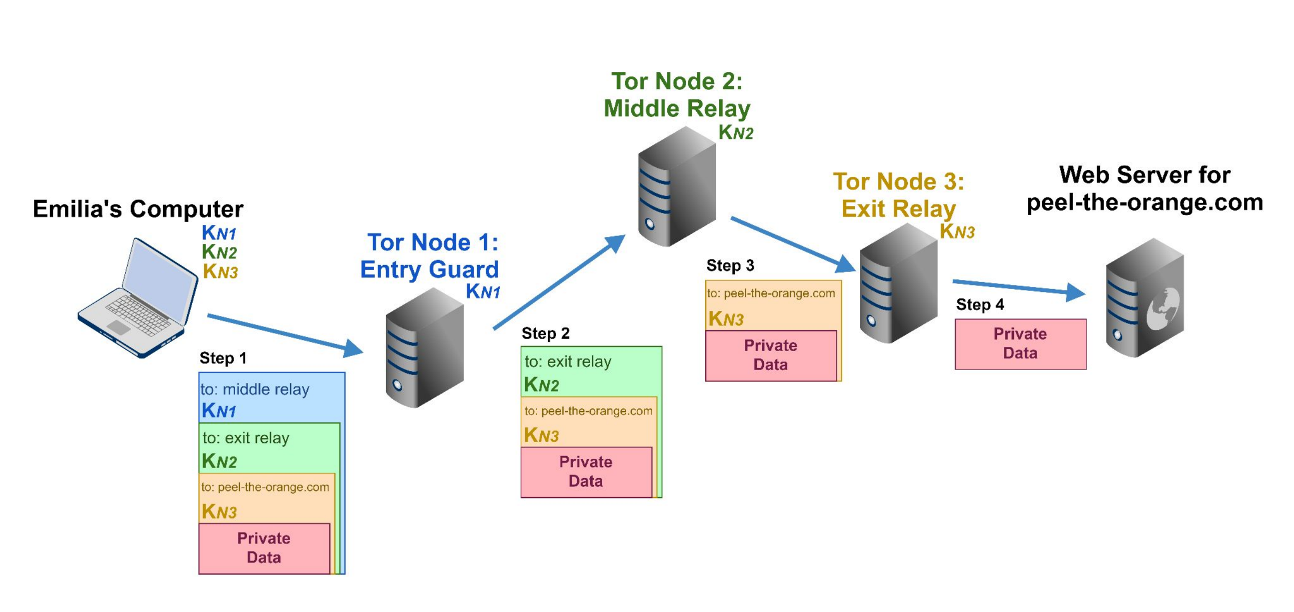
- They can just subpoena the VPN provider's logs and figure out who was connecting to what site at what times
- Some VPNs claim not to store logs (notably Proton and Nord)
    - They still have to cooperate with law enforcement. Wiretap orders, gag orders, subpoenas, etc. remain in effect
- VPNs can help protect you from corporate surveillance. They can't do much against state actors.

Background | Crime time again

- **Criminals cannot trust any centralized system** or organization, including ISPs, VPNs, etc.
- The only way to hope to have security is to have a mostly decentralized communication relay system
- This is where **The Onion Router (TOR)** comes in

Tor: Basics

- Instead of relaying all our traffic through one centralized entity (e.g. VPN), we will relay it through a whole bunch of randomly selected nodes, all run by volunteers.
- Data is encrypted in layers (hence “Onion”)
- **There is no single node which knows both who you are and who you’re talking to**



Tor: Relay selection

1) Client queries a hardcoded list of Directory Authorities for a list of Tor relays
   a) Authorities vote to establish consensus and sign a list
2) Client selects relays (possibly at random) and negotiates a key with each of them (like in TLS)
3) Client then uses these relays to construct a Tor **circuit**, using their keys to encrypt messages in layers.

Tor: Entry Guards

Selecting all nodes purely randomly has a problem: If an attacker controls some malicious nodes for long enough, if you use Tor long enough eventually you will stumble upon one of their nodes.

Each client selects a small list of entry nodes and only uses those. The idea:

- If the attacker doesn’t control those, all is good forever
- If the attacker does control those, they can see a larger fraction of your traffic, but that doesn’t make things considerably worse

Bonus effect: Somebody can’t just set up 5 Tor nodes and eventually get a list of every single IP which uses Tor

Fed time part 2

Those pesky criminals have obscured their IP addresses when browsing to their crime websites! What do we do now??

- Take down the websites
    - Send subpoenas to the ISPs, DNS providers, Bill Gates’s grandma, etc. etc.
- What if a criminal wants to *run* a website anonymously?

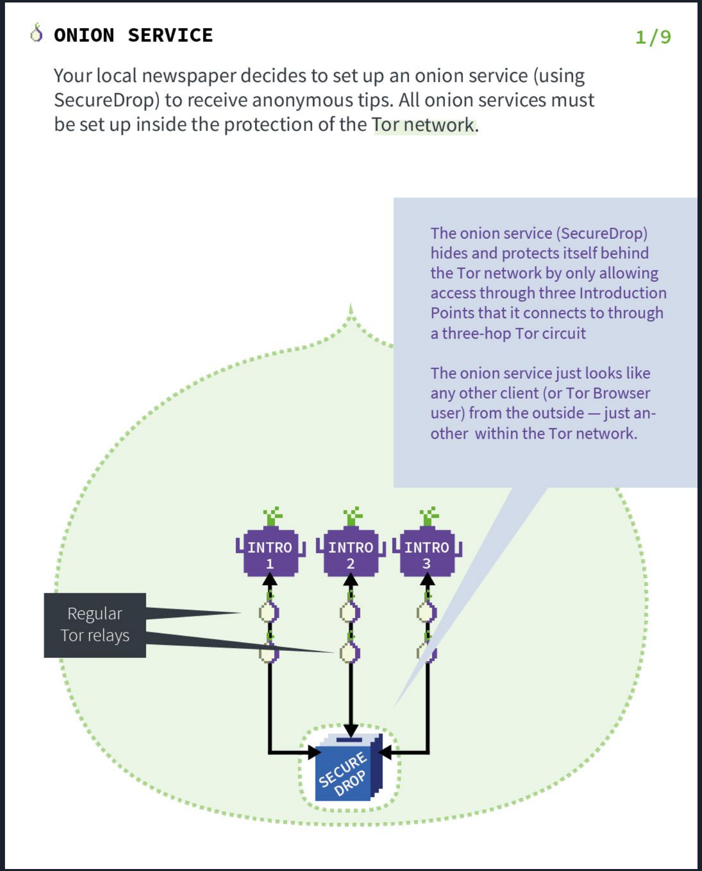
This is where **Onion Hidden Services** enter the picture

The Dark Web (Finally)

Hidden Services / Onion Services are a way for servers to sit within the Onion network and appear to be ordinary clients.

An HS signs its intro points with its private key and publishes that into the directory, which clients can then query. **Public key is stored in address of the service**.

Client selects rendezvous point and sends that through intro node to HS.



ONION SERVICE

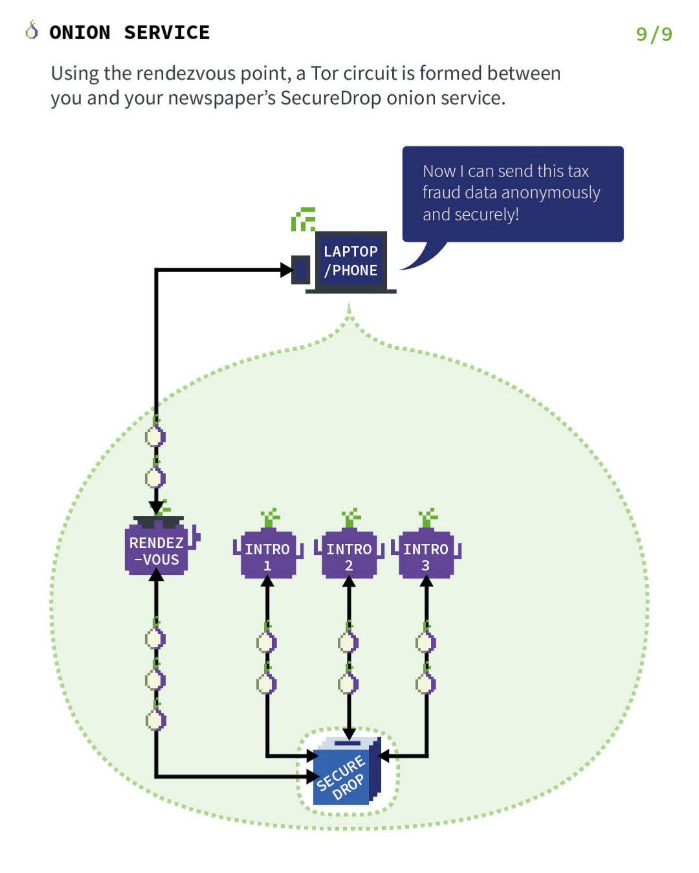
1/9

Your local newspaper decides to set up an onion service (using SecureDrop) to receive anonymous tips. All onion services must be set up inside the protection of the Tor network.

The onion service (SecureDrop) hides and protects itself behind the Tor network by only allowing access through three Introduction Points that it connects to through a three-hop Tor circuit

The onion service just looks like any other client (or Tor Browser user) from the outside — just another within the Tor network.

The Dark Web (Finally)



ONION SERVICE 9/9

Using the rendezvous point, a Tor circuit is formed between you and your newspaper's SecureDrop onion service.

Now I can send this tax fraud data anonymously and securely!
LAPTOP /PHONE
RENDEZ -VOUS
INTRO 1
INTRO 2
INTRO 3
SECURE DROP

Now a client can connect to a server without having any way of knowing that server's IP! This server is now on the **dark web** - it can *only* be accessed through Tor, and nobody knows where it is or who runs it.

…at least in theory. Server owners sometimes fuck up: https://sh1ttykids.medium.com/new-techniques-uncovering-tor-hidden-service-with-etag-5249044a0e9d

A more in-depth overview can be found at https://community.torproject.org/onion-services/overview/

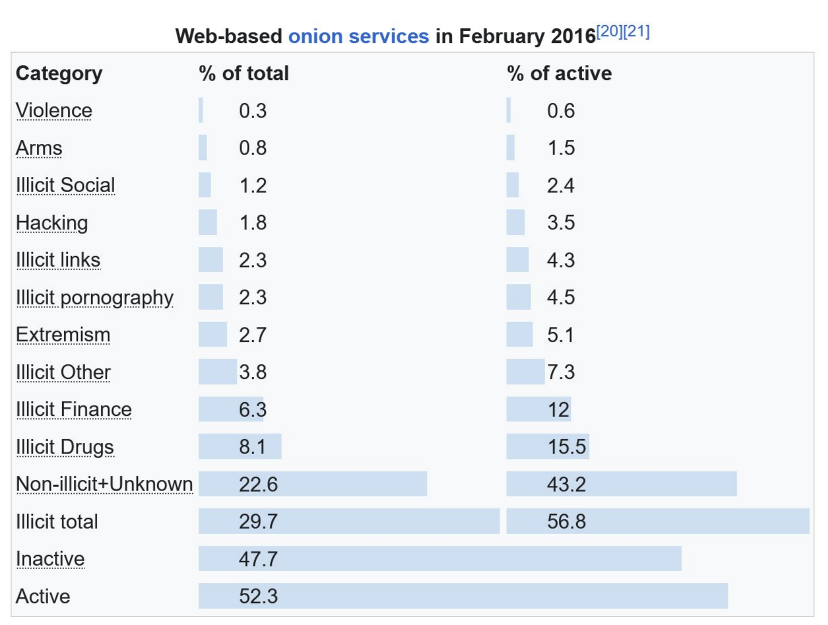
Further reading

What we just covered is like 0.1% of the Tor spec. I highly encourage skimming the spec itself - https://spec.torproject.org/tor-spec/ - it talks about some cool things and even cooler attacks that they try to mitigate against.

What is Tor used for?

Hidden services: Basically just crimes lmao

The rest of Tor: Still mostly crimes



Web-based onion services in February 2016[20][21]

Category	% of total	% of active
Violence	0.3	0.6
Arms	0.8	1.5
Illicit Social	1.2	2.4
Hacking	1.8	3.5
Illicit links	2.3	4.3
Illicit pornography	2.3	4.5
Extremism	2.7	5.1
Illicit Other	3.8	7.3
Illicit Finance	6.3	12
Illicit Drugs	8.1	15.5
Non-illicit+Unknown	22.6	43.2
Illicit total	29.7	56.8
Inactive	47.7	
Active	52.3	

Ethical Uses for Tor

- Whistleblowers:
  - https://securedrop.org/
- Citizens in authoritarian countries who have restricted internet access
  - Many of these regimes try to block Tor itself for obvious reasons! This leads to an arms race between Tor and various governments; see https://www.youtube.com/watch?v=YIZZQYLIXe8
- Citizens in authoritarian countries who have restricted access to abortions, contraceptives, medication for trans folks, etc.
- **All of these are still crimes!**
- Non-crime use case: Avoiding surveillance from Google/Facebook/TikTok/etc.
  - Or masking your identity from scammer sites, Russian government sites, etc.

Hidden Service Examples

Legit:

- ProPublica: http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/
- New York Times: https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/
- Facebook: http://facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/
  - Used by over a million people!
- Reddit: https://www.reddittorjg6rue252oqsxryoxengawnmo46qy4kyii5wtqnwfj4ooad.onion/
- Amnesty International: https://www.amnestyl337aduwuvpf57irfl54ggtnuera45ygcxzuftwxjvvmpuzqd.onion/
- CIA (lmao): http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion

Hidden Service Examples

Actual dark web stuff:

- BreachForums: http://breached26tezcofqla4adzyn22notfqwcac7gpbrleg4usehljwkgqd.onion
- OmniForums: http://onnii6niq53gv3rvjpi7z5axkasurk2x5w5lwliep4qyeb2azagxn4qd.onion/
- dark.fail: http://darkfailenbsdla5mal2mxn2uz66od5vtzd5qozslagrfzachha3f3id.onion/
- Onion search engine: https://ahmia.fi/ / http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/

Known attacks against Tor users

- Spin up a shit ton of nodes and hope that you control both an entry and an exit node
- Wait for someone to download a large file without using Tor
  - https://www.usenix.org/events/leet11/tech/full_papers/LeBlond.pdf
- Traffic correlation/analysis
  - If you know that someone connected to Tor at [x] time, and right after that a Tor node talked to drugskejwhgkjgwhkjhg.onion, you can make a pretty good guess as to what happened there
- Consensus attack (compromise a majority of the directory authorities)

Known attacks part 2

Fingerprinting:

- A website can use a client’s screen resolution, system fonts, user agent, etc. to very accurately “fingerprint” them (build a unique profile on them)
- Tor ignores system fonts, always boots up in the exact same resolution, and removes unnecessary user agent data to protect against this.
- There are probably tons of other cool side-channel attacks you can do to fingerprint though! E.g. system resources, connection speeds, etc. Research this :)