

Encrypted drives, Signal, VPNs and
Tor Oh My!



Encrypted Drives

- Often the drives of your computer or phone are left unencrypted & anyone can attach them to another computer and read them
 - Such as a border guard
- Enabling drive encryption prevents that when you have turned off your computer or phone

Encrypted Drives

- Drive encryption is on for iPhones
- You need to turn it on for most other phones and Windows, MacOS and Linux computers
- Reminder: only works when the computer has been turned off, not when it is asleep

Signal

- A free secure text, voice and video communication application
- Works for Android, iPhone, Mac & Windows
- WTF! No Linux????
- Find it at signal.org
- Paid for by donations

Signal

- Signal messages and calls are end-to-end encrypted, which means that they can only be read or heard by your intended recipients.
- The Signal service does not have access to the contents of any messages or calls sent or received by Signal users.

Signal

- How do we know?
- Their client and server source code is available for anyone to look at and find insecurities
- Also, the app makes it very easy to verify the keys of the people who you talk with. If their key changes (get a new phone say), it warns you so you can reconfirm their key, perhaps in person.

Signal

- Let's try it out!

Virtual Private Networks (VPNs)

- VPNs take the data you send out on the internet, encrypt it and send it to somewhere else to get on to the Internet
- Most useful when you don't trust the local WiFi network, such as at cafes or events.
 - Also, when you don't trust your ISP not to monitor you or inject ads into the insecure websites you visit
- Often used to provide secure access to a work network

Virtual Private Networks (VPNs)

- Why else? Getting around country copyright blocks. Want so see BBC shows for free? Get a VPN the exits in the United Kingdom.
- Traveling, but want to watch a US streaming service or play a US game, get a US VPN that exits in the US.

Virtual Private Networks (VPNs)

- Usually you would use a monthly service. Your choices are free to expensive, but of course nothing is free so check out what data they gather.
- Check them out at ThatOnePrivacySite.net. Click on the VPN Section.

Virtual Private Networks (VPNs)

- Let's try one out:
 - whatismyip.com or maxmind.com/en/geoip-demo
 - Local
 - With VPN

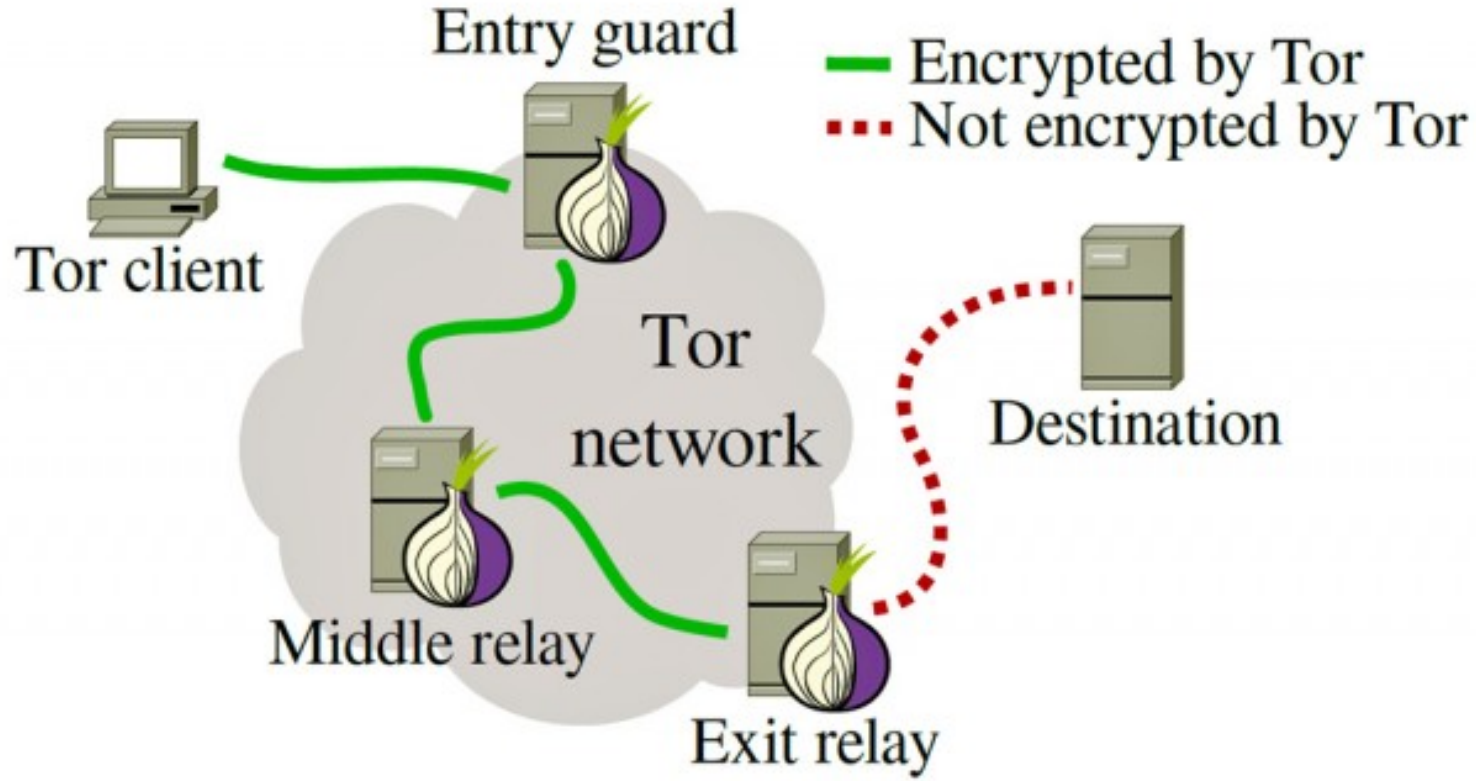
Tor

- Tor was setup by the US Navy so their spies could access US Navy sites in other countries without the local country being able to monitor or stop them
- Since spun out into the Tor Project
- Still gets a lot of funding from US government
- Last we knew the NSA hadn't broken it

Tor: How it Works

- Tor Browser Bundle merges Firefox with the Onion router and is easy to setup
- Why reinvent the wheel. Let's look at Steve Revilak's Massachusetts Pirate Party Tor presentation:
 - <https://masspirates.org/blog/wp-content/uploads/2015/01/tor-20150110.pdf>

Tor: How it Works Review



Tor Limitations

- Tor is slower than using an ordinary web browser so don't torrent over it.
- Web sites that rely heavily on Geolocation (e.g., Google) might get confused about your “unusual location”.
- It won't save you if you login to a site with an account you use outside of Tor.

Tor Limitations

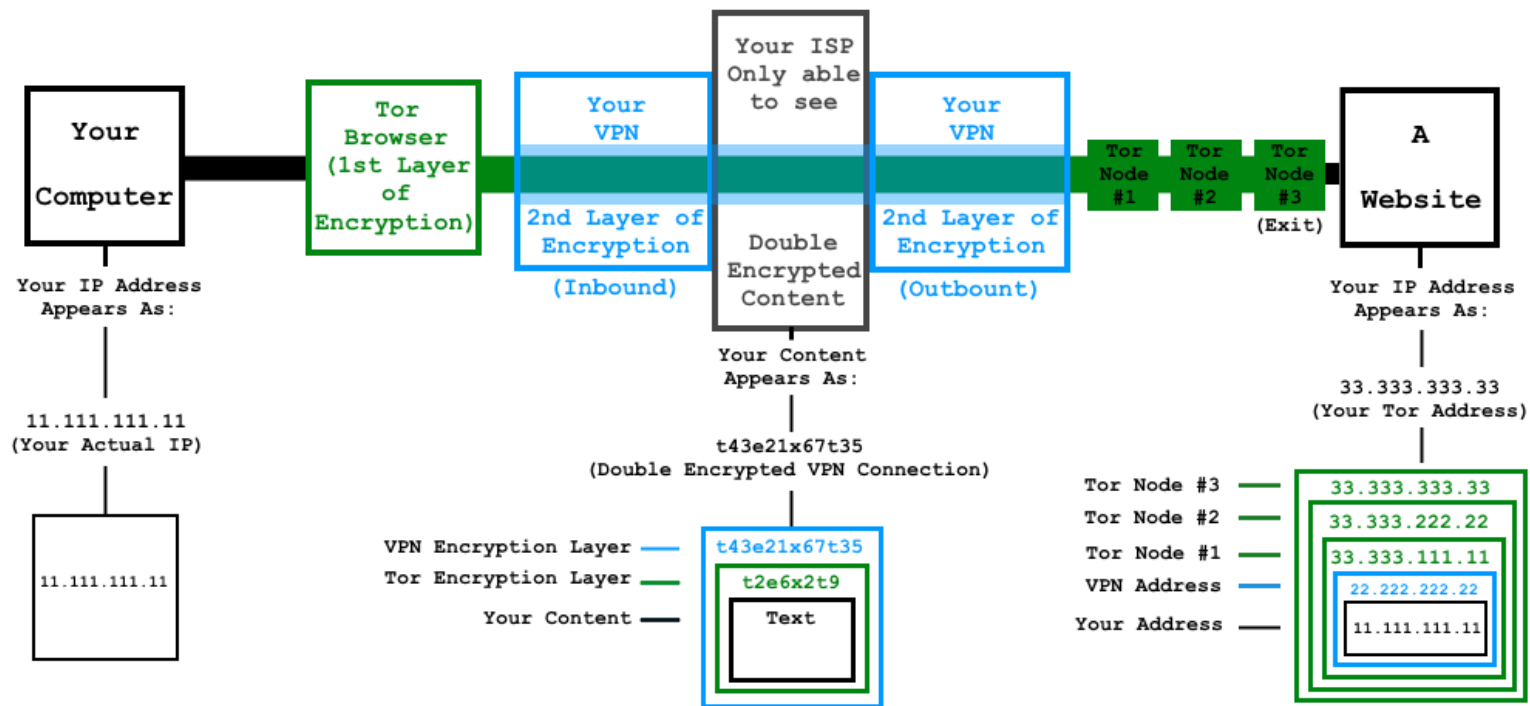
- You will need to change your browsing habits:
 - Don't enable or install browser plugins
 - Use the HTTPS versions of websites (should do that everywhere, actually)
 - Don't open documents downloaded through Tor while online as it could phone home and identify you
 - Try changing the size of your browser window each time you use Tor. Sites will fingerprint you from your browser window size among other browser characteristics.
 - Reminder: don't login to sites with credentials you use outside Tor and don't login with an email that you use outside of Tor.

Tor

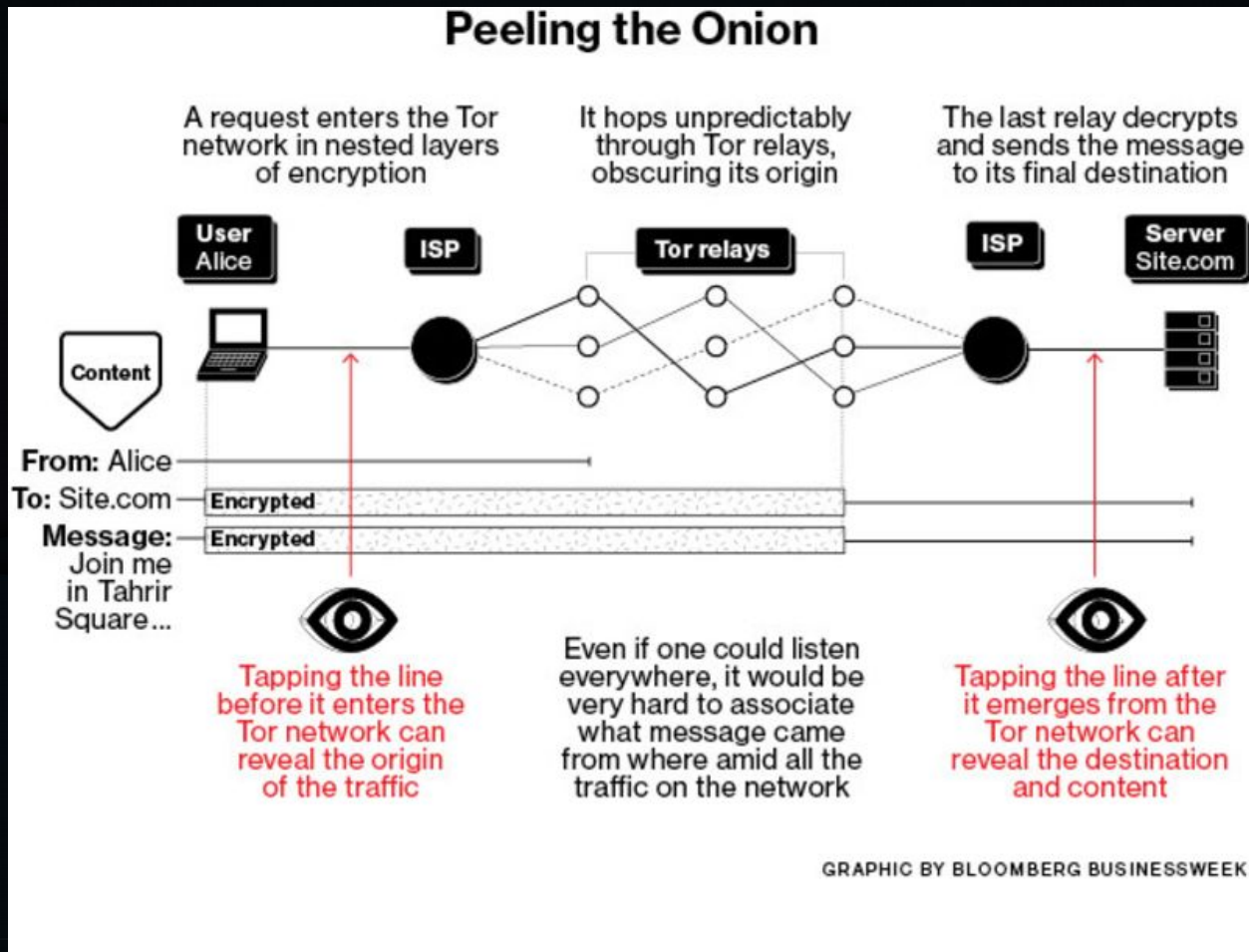
- Get it at [TorProject.org](https://torproject.org)
- Let's try one out:
 - whatismyip.com or maxmind.com/en/geoip-demo
 - Local
 - With VPN
 - What if we change our circuit?

Tor & a VPN

VPN + Tor Network Map



Tor: Trying to Break It



Tor Hidden Services

- Tor Hidden Services provide an extra layer of protection by sending your traffic to a site from inside the Tor network
 - ... and never on the Internet
- Tor hidden services have a special domain that only works in Tor.
- Often used by “Dark Sites”, but even Facebook has a Tor hidden service: `facebookcorewwi.onion`

Tor Summary

- Using Tor is just as easy as using any other web browser.
- Tor protects you from surveillance by proxying web traffic through a network of Tor nodes.
- The network of Tor nodes conceals your location; encryption protects the content of your traffic.

