**VPN Weaknesses**

Slower than ISP alone as adding extra layer of encryption and extra hop

VPNing out of the country makes speed and latency worse

* Faster than alternatives though such as Tor, I2P and JonDoNym

**A single VPN alone is not suitable to hide your identity from a motivated nation state**

* **Only when used in combination** with other VPNs nested, or with Tor or JonDoNym for a high-level adversary

A censor can use firewalls that the VPN is going through, using DPI to determine if the encryption being used is that of a VPN

Probes can also be used on suspected VPN servers to determine if it’s a VPN

**OpenVPN and IPsec protocols are both distinctive from HTTPS so its possible to see the difference**

* **Connection can be blocked, but still not seen or understood**

Money trail unless done anonymously

**To change geographical locations**

* HTTPS
* SOCKS5 proxy
* Web proxy

**Low latency anonymising service**

* Need traffic to get to dst quickly and come back quickly
* Need a quick response
* All LLASs are susceptible to traffic conformation or e2e correlation attacks
* Due to VPN services having a relatively small number of servers located in a few data centres with a small number of users per server, a high-level adversary could cross-correlate all the entry and exit conversations
  + Would be less tan a million comparisons for an average VPN service which is trivial for a nation state
* They are also susceptible to active attacks
  + If the adversary can observe (not see unencrypted) traffic between the user and VPN server, they could affect it in some way and make correlations based of that
  + Send too many packets to VPN server
    - They could see difference in impacts to the user’s online activity, time variations, changes in connection to the server which would help deanonymize the user
* Don’t protect you from client attacks
  + If the destination server/website has been exploited with a code injection and your client executes the code by clicking on an image for example then a VPN won’t protect you against that
* Web traffic fingerprinting
  + Looks at size and timing of encrypted data streams
  + The adversary can still guess what webpage is being visited because each webpage has a different pattern of traffic
  + Although the content isn’t viewable, the name of the website you’re accessing is no longer private
  + 90% accuracy on identifying HTTP packets on conventional VPN protocols
    - OpenSSH and OpenVPN required a larger amount of data before HTTP packets were identified
* Occasional VPN usage
  + If you don’t run your VPN constantly, then it will show that you are trying to do something private when you do use the VPN
* VPNs can be blocked by certain websites like Netflix
* If used for different aliases at the same time, this could contaminate them
* CAPTCHAs
* Don’t filter or replace TCP packets so not protected from TCP timestamp attacks
* Lack of a hardened browser unlike Tor or JonDoNym
  + VPN sessions can still be tacked from site to site
  + Browser fingerprinting, browser exploits, cross site tracking, cookies, referrers etc.

**They are more a tool for privacy than for anonymity**

* To protect anonymity, they cannot know your source IP, payment details or anything about you, but they will
* Only possible to get full anonymity via VPNs when using nested VPNs or other anonymising services in conjunction

**Can you trust VPN providers?**

**VPNs are like dogs, even if you get a pedigree, there’s always the chance that one day it might turn around in a bad mood and bite you**

To connect to a VPN, you must reveal your real IP address to the VPN provider

* The provider is a MITM and could therefor perform such attacks if they wanted or were coerced
* They could log all your traffic
* A bad VPN service is no different to a bad ISP
* They can be served with court orders forcing them to disclose info

EU has data retention/logging laws

US don’t

* Although VPNs are known to be targeted by nation states to co-operate in deanonymizing their users

**Avoid using servers based in the 5 or 14 eyes**

**Can never fully trust VPN providers**

* **Could even bet that some of the nation states even run some of these VPN services**

**Must distribute the trust**

* Collusion between multiple parties would be necessary to compromise your identity which is harder than the single entity that is one VPN service
* This means using nested VPNs, hotspots, nested Tor etc.