**Introduction to VPNs**

**There are many anonymising services like VPNs:**

* TOR
* JonDoNym
* SSH tunnels
* Proxies
* Freenet
* I2P

**VPNs work by creating an encrypted tunnel for your traffic to go through to their server**

**Then the server routes the traffic through to the exit node, unencrypted**

**Types of VPN protocol**

* Point-to-point Tunnelling Protocol (PPTP)
* Layer Two Tunnelling Protocol (L2TP)
* Internet Protocol Security (IPsec)
* OpenVPN
* Secure Socket Tunnelling Protocol (SSTOP)
* Internet Key Exchange (IKEv2)
* SoftEther
* OpenConnect

**PPTP**

* MS chat which uses this has been subject to many attacks
* Even Microsoft doesn’t recommend using it
* Nation states or high order adversaries are very likely to be able to decrypt PTP
* Last last resort

**LT2P/IPsec**

* Usually integrated with IPsec
* Doesn’t provide encryption of the traffic
* Most modern OS natively support
* Use fixed ports and protocols which make it inflexible unfortunately
* More easily blocked by NAT firewalls
* May require port forwarding if behind a firewall
* Much easier to block than OpenVPN due to reliance on fixed open ports
* Not viable for high order adversaries
* Uses AES so ill protect against hackers and low-level adversaries

**OpenVPN**

* Open source
* OpenSSL library, SSL v3.0, TLS V1
* Processes and ports are configurable
* Can use either UDP or TCP
* Could set up to emulate normal HTTPS web traffic by configuring for port 443 on TCP
  + Makes it difficult to tell a VPN is being used instead of normal traffic
  + Works faster over UDP though obviously
* AES, RSA, DHEC, Blowfish, RC2/4/5, Camellia
* Not natively supported by most OS
* Need free 3rd party software to install
* No evidence that Nation states have comprised OpenVPN
* In SSL/TLS mode, the session keys are periodically changed to promote forward secrecy
* Encryption algorithms that you want to see
  + 2048-bit pr 4096-bit RSA certificates
  + DHE-RSA-ARS256-SHA for exchange of OpenVPN key material
  + AES-256-CBC-SHA for data
* **Use whenever possible with above mentioned configurations**

**SSTP**

* Proprietry standard by MS
* Offers many advantages of OpenVPN but particularly for Windows
* Not open source
* Don’t trust Microsoft

**IKEv2**

* Jointly developed by Cisco and MS
* Enhanced ability to reconnect when connection is dropped
* Good for mobiles for quick and easy solution
* Reasonably secure and fast
* Better to use OpenVPN unless reconnection is better than privacy