**SSLs and TLSs**

**Secure Sockets Layer & Transport Layer Security**

Cryptographic (encryption) protocols designed to give communication security over a network or the internet

* SSL is the older encryption protocol and TLS is the new one

Many sites still use SSL for compatibility

TLS is used in HTTPS, can be used with VPNs and FTP and many other protocols

**TLS gives**

* Confidentiality
* Authentication
* Integrity

**Diffie-Helman key exchange**

Forward Secrecy

* Gives assurance that your session keys won’t be compromised even if the public key of the server is compromised
* By generating a unique session key for every session a user initiates
* This means that only the information in that one single session (not all data) will be compromised if the session key is compromised too

If private keys for server are compromised, then all previous messages sent on the server can’t be decrypted due to using Diffie-Helman to generate different session keys that are only used for a short time

TLS 1.3 is the newest version of the TLS protocol

* Newest most secure but also not compatible with most
* TLS 1.0 is often used instead

**Ciphersuite**

This is the combination of encryption algorithms used

* Mozilla.org
* weakDH.org
* GRC.com
* Ciphersuite list in order of strength

**SSL Stripping**

Two ways to connect to Https

* Type in the domain and the server will perform a 302-redirect which will then redirect you to the https version of the site
* Via a link (on google) will directly take you to a https version

SSLstrip acts a proxy looking for those two events

* Changes https connections to http connections

Methods

* Wifi pineapple
  + Hardware device that sets up a malicious access point for you

Defences include

* Arpwatch for arp spoofing/poisoning
* Sniffer detection
* Tunnelling (SSH, VPN etc)
* Browser settings to only allow https connections
* VLANs
* firewalls