**Module 2 Technologies & Tools**

**2.6 Security Protocols**

**Security Protocols – Web**

* SSL (Secure Sockets Layer) – Latest version 3.0

1. Now depreciated by IETF
2. Uses certificates for authentication & encryption for message integrity & confidentiality
3. Establishes *stateful connection*

* TLS (Transport Layer Security)

1. Based on SSL v3.0
2. Provides privacy (Symmetric encryption), message integrity (Message Authentication Code) & authentication (PKI digital certificates)
3. *Forward secrecy* ensuring any future disclosure of encryption keys cannot be used to decrypt any TLS communications recorded in past

* HTTPS (Hyper Text Transfer Protocol Secure)

1. Uses SSL/TLS to secure web-based communications
2. X.509 digital certificates
3. 256-bit encryption keys

**DNSSEC (Domain Name Service Security)**

* Suite of Internet Engineering Task Force (IETF) specifications
* Review how DNS works from earlier sections
* Protects against DNS Cache Poisoning
* DNS extensions provide DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence & data integrity (not confidentiality or availability)

**SSH (Secure Shell)**

* Replaces Telnet for remote communications
* Establishes session between client & host computers using authenticated & encrypted connection
* Uses asymmetric (public key) RSA (Rivest-Shamir-Adleman, it’s actually named after it’s creators) cryptography for both connection & authentication
* Used for remote administration of Linux servers
* Other protocols can tunnel through SSH

**Secure Email**

* Secure/Multipurpose Internet Mail Extensions (S/MIME)

1. Standard for encryption (confidentiality) & signing (authentication) of MIME (email) data
2. Requires PKI & uses Certificate Authorities (CA)
3. Internal email

* POP3S (Post Office Protocol Ver3 Secure) & IMAPS (Internet Message Access Protocol Secure)

1. Use SSL to secure emails in transit between POP/IMAP server & client
2. External email

**FTPS (File Transfer Protocol w SSL/TLS)**

* FTP passes credentials in clear text
* FTPS – FTP extension that uses SSL/TLS

1. Mutual authentication of parties (certificates)
2. Data confidentiality (encryption) & integrity (hashing)
3. FTPS implicit over port 990
4. FTPS explicit over port 21

* SFTP (Secure FTP) – uses SSH to transfer files (SSH encapsulation)

**SRTP (Secure Real-time Transfer Protocol)**

* Secure voice & video transmissions
* Voice & video calls established with Session Initiation Protocol (SIP) & data transmitted with Real-time Transfer Protocol (RTP)
* Is an extension to RTP
* Intended to provide encryption, message authentication & integrity & replay attack protection to RTP data in both unicast & multicast apps

**LDAPS (Lightweight Directory Access Protocol over SSL/TLS)**

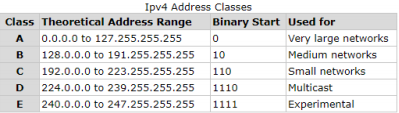
* LDAP is a Directory Protocol – contains sensitive information about organisational systems & users
* Attackers may sniff network to read unencrypted LDAP traffic
* LDAPS over SSL/TLS
* Uses TCP port 636

**SNMPv3 (Simple Network Management Protocol Ver3)**

* SNMP used to manage networks
* Each managed device has software agent reporting configuration settings & alerts (traps) to central SNMP management server
* SNMPv1 & v2 all sent data as clear text
* SNMPv3 encrypts data

**Use Cases – Network Address Allocation**

* Allocating IP addresses
* DHCP (Dynamic Host Control Protocol) – assigns internal IP addresses
* Use of network subnets to segregate multiple hosts & control network traffic



**Use Cases – Time Synchronisation**

* NTP (Network Time Protocol) – UDP protocol used to synchronise time based on atomic clock
* NTP servers – redundant & secured

**Use Cases – Subscription Services**

* Software as a Service (SaaS)
* Cloud Email – Google Gmail & Microsoft Office 365
* Network defences

1. Firewall/IDS/IPS
2. Web & app filtering
3. Antivirus/Malware detection
4. Patching