5. Security

17.1 Encryption, Encryption Protocols and Digital Certificates

Key Cryptography

- Ensures a message is authentic/from a trusted source
- Ensures message has not been altered during transmission
- Makes sure only intended receiver is able to understand a message
- Non-repudiation – neither sender or receiver can deny the transmission happened

Asymmetric Encryption

- Provides better security – by using a pair of different keys
- One of the keys is used to encrypt the message, the matching one is used to decrypt it
- Only the public key is available to everyone, the private key is kept secret
- Is a longer process, as it is more complex
- Length of keys is longer (usually 2048 bits)

Process

- The receiver's computer uses an algorithm to generate a matching pair of keys (public and private)
- The public key is sent to the sender's computer
- The sender encrypts the document/file/data using the public key to create cipher text
- The sender's computer sends the cipher text to the receiver's computer – can only be decrypted using the receiver's private key

Detecting Alterations

- The message, together with the digital signature, is decrypted using the receiver's private key
- The digital signature received is decrypted with the sender's public key to recover the digest sent
- The decrypted message received is hashed with the agreed hashing algorithm to reproduce the message digest received
- The two digests (received and reproduced) are compared – if they are the same, then the message has not been altered

Symmetric Encryption

- Uses a single key which is used/shared by all to encrypt and decrypt messages
- Simple process that can be carried out quickly - risk of compromise is higher
- Length of keys is shorter (usually 128/256 bits)

Quantum Cryptography

- Protects security of data transmitted over fibre optic cable
- Is a virtually unhackable encryption system

Benefits

- Detects any eavesdropping (due to change in photon properties)
- Once transferred, the integrity of the key can be guaranteed – it cannot be copied or decrypted later
- More secure, longer keys can be used

Limitations

- Limited range – works only over relatively short distances
- Requires a dedicated fibre-optic line and specialist hardware – is expensive
- Polarisation of light may be altered during transmission through fibre-optic cable
- Lacks many vital features and has high error rates (still new and being developed) – e.g. digital signatures, certified mail etc.

Private Key

- An unpublished/secret key that is never transmitted anywhere
- Has a matching public key
- Is used to decrypt data that was encrypted with its matching public key

Purpose and Example Situations of SSL/TLS

Secure Socket Layer

- *Encrypts data being transferred over the internet – decides on which encryption algorithms are to be used*
- *Performs data integrity checks and data compression*

Transport Layer Security

- *Provides encryption, authentication and data integrity in a more effective way than SSL*
- *Ensures privacy and security of data between devices communicating over the internet – provides third-party eavesdropping*

Examples of where SSL/TLS would be used

- *Online banking and online financial transactions*
- *Sending and receiving emails, sending software to a restricted list of users*
- *Using cloud storage facilities or a VPN*

SSL/TLS use when Client-Server Communication is Initiated

- A SSL/TLS connection is initiated by an application which becomes the client
- The application which receives the connection becomes the server
- Every new session begins with a handshake
- A digital certificate is requested/sent from the client/server
- The client verifies the server's digital certificate and obtains the server's public key
- The encryption algorithms are agreed upon by the server and client – the symmetric session keys are then generated

Digital Certification

Digital Signatures

- An enquiry is made to Certificate Authority (CA)
- The enquirer sends their public key and all required information (e.g. to prove identity) to CA
- The enquirer's details are checked by the CA – If details are verified then the public key is agreed upon
- The CA creates/issues a certificate that includes the enquirer's public key
- Encrypting data is sent to the CA using their public key and sent by the CA using their private key

How it's produced before a message is sent

- Message is hashed using the agreed hashing algorithm to produce a digest
- The message digest is then encrypted with the sender's private key to form the signature

Digital Certificate

- An electronic/online document used to authenticate the identity of a website/individual/organisation
- Typically issued by the CA
- Contains information for identifying an individual/website owner and a public key
- Provides the public key which can be used to validate the private key associated with the signature