2. Secure socket layer(SSL) and Transport layer security(TLS)

Purpose:

- The SSL & TLS provide communication security over the internet/network
- … they provide encryption
- They enable two parties to identify and authenticate each other
- … and communicate with confidentiality and integrity

Situations where the use of SSL/TLS would be appropriate:

- Online banking and all online financial transactions
- Online shopping/commerce
- Sending software to a restricted list of users
- Sending and receiving emails
- Using cloud storage facilities
- Intranet, extranet, and internet
- Using virtual private networks (VPNs)
- Using Voice over Internet Protocol (VOIP) for video and audio chatting over the internet
- Using instant messaging
- Making use of a social networking site

Difference between SSL and TLS

- It is possible to extend TLS by adding new authentication methods
- TLS can make use of session caching which improves the overall performance of computer compared to using SSL
- TLS separate handshaking process from record protocol layer

SSL

- Encrypts the data when the user logs onto a website
    - Only the client's computer and the web server are able to make sense of what is being transmitted

- Data compression: reducing the amount of data being transmitted
- Data integrity checks

TLS

1. **Record layer** can be used with or without encryption; it contains the data being transmitted over the internet
2. **Handshake protocol** permits the web server and client to authenticate each other and to make use of encryption algorithms (a secure session between the client and server is then established)
    - Cipher suite
3. **Session caching** avoids the need to utilize computer time during each TLS connection; TLS can either initiate new session or resume existing session; the latter can save considerable computer time

- A protocol with two layers
    - Handshake and Record layers
- A TLS/digital/public key certificate is used for authentication
- Handshake uses asymmetric cryptography
    - To generate agreed paramters
    - Establish a shared session key
- The shared session key provides symmetric cryptography for sending a receiving data(record layer)
- At the end of the session, all the paramters, keys, etc. are erased

Situations where the use of TLS would be appropriate:

- Browser accessing secure websites. eg: bank transaction
- VPNs - Virtual private networks
- VOIP - Voice over Internet Protocols
- Email

Describe the type of activity where SSL or TLS would be used

- A client
- … is accessing a website
- … and needs to communicate with the website
- … without the possibility that the communication being intercepted or scrutinized by an unauthorized party

- … because sensitive data is being transferred

Past paper questions

1.

Problems that SSL/TLS helps to overcome:

- Security: alteration of transmitted message
- Privacy: only intended receiver can view data
- Authentication: trust in other party

Security parameters agreed during the handshake process:

- Which protocol will be used
  - There are a number of different versions of the two protocol
- Session ID
  - Uniquely identifies a related series of message between the client and server
- Session type
  - Reusable or not
- Encryption method
  - public/private key to be used
- Authentication method
  - Use of digital certificates
- Compression
  - … methods to be used

3.

Explain how SSL/TLS protocols are used when a client-server communication is initiated.

- An 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 (as defined in the SSL/TLS protocols)

- The client requests the digital certificate from the server // The server sends the digital certificate to the client
- The client verifies the server’s digital certificate
- And the obtains the server’s public key
- The encryption algorithms are agreed
- The symmetric
- … session keys are generated

4.

The sequence of steps describes what happens when setting up a secure connection using Secure Socket Layer (SSL)[1]

- Browser requests that the server identifies itself
- Server sends a copy of its SSL Certificate and its public key
- Browser checks the certificate against a list of trusted certificate authorities
- If the browser trusts the certificate, it creates, encrypts and sends the server a symmetric session key using a server’s public key
- Server decrypts the symmetric session key using its private key
- Server sends the browser an acknowledgment, encrypted with the session key.
- Server and browser now encrypt all transmitted data with the session key

---

1. Q4 is a more detailed version of Q3↩