Security Protocols

IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Q1-5 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. What is the place of TLS in the TCP/IP network stack?

   TLS sits between the application layer and the transport layer.

2. What are the tasks of the TLS handshake and the TLS record protocol?

   TLS Handshake establishes the security association and the shared secret key to be used for encrypting the actual traffic. TLS record is the actual transport part, where the new shared key is used to encrypt packages.

3. What is the role of `ChangeCipherSpec` message in TLS record protocol?

   It triggers the record protocol to start encrypting the traffic using negotiated keys and algorithms. The `ChangeCipherSpec` must be sent by both sides (client and server) for TLS record protocol to start encrypting the traffic.

4. How TLS prevent the man-in-middle attack?

   Diffie-Hellman Key Exchange is vulnerable to Man-in-middle attack as the attacker can impersonate the server to start key exchange with the client. To tackle this, certificate in TLS sets up a trust system to certify the public key is from the authentic server. The certificate of the server is signed by a certificate authority, a renowned organization such as Microsoft.

   Client verifies the signature on the certificate is from the trusted organization and so trusts the server is authentic.

   And, the attacker is unable to forge the signature of a trusted organization.

5. IPsec operates at which layer of TCP/IP protocol stack?

   Network layer.

6. What is the difference between Authentication Header and Encapsulating Security Payload protocols of IPsec?

   From RFC 4301 `https://tools.ietf.org/pdf/rfc4301.pdf#19`:

   - AH: offers integrity and data origin authentication, with optional (at the discretion of the receiver) anti-replay features.
   - ESP: offers the same set of services as AH, and also offers confidentiality.

7. What is the difference between Tunnel mode and Transport mode of ESP?

   In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets.

8. Explain why a VPN in most cases does not provide end-to-end encryption.

   Encryption is usually between VPN client (software) and VPN gateway or between two VPN gateways. Traffic will be in clear in the internal network behind the gateway(s) and also on the client side, an attacker can get access to the information before it is encrypted (or after it is decrypted).

   In rare cases the VPN is used between two end-point hosts in which case end-to-end encryption is provided. This however is rather inconvenient if one of the hosts is providing a public service such as web.

9. Explain the purpose of the numeric comparison or passkey entry association models in the Bluetooth LE Secure Connections protocol.

   The purpose is to allow the two devices A and B that intend to communicate securely to verify via an authenticated channel (i.e. via the human user) that they are really talking to each other, to prevent Man-In-The-Middle (MITM) attacks where A and B are each talking in two separate sessions to an attacker M rather than to each other. For example, for numeric comparison model, in the case of the MITM attack, the number displayed at device A (which is derived from the shared of key of M with$A$) would not match the number displayed at device B (which is derived from the shared key of M with B) so the numeric comparison will fail.