EBU7140

Tutorial 4

2020

1) Explain the protocols included in TLS architecture

- Handshake protocol
- Change cipher spec protocol
- Alert protocol
- Record protocol
- Heartbeat protocol

*And **explain** each protocol*

2) What are the definitions of TLS connection and TLS session?

- A connection in TLS is a transport that provides a suitable type of service. The connections are peer-to-peer relationships and are transient. Every connection is associated with one session.
- A session in TLS is an association in between a client and a server. They define the security which can be shared between multiple connections (to avoid expansive renegotiation of security parameters).

3) How does PGP provide authentication and confidentiality? You may want to use a diagram to illustrate it.

See lecture Slides

4) How many types of encryptions keys are used/generated in PGP?

- Pass-phrase key
- Session keys (random keys generated)
- Public-key
- Private-key

5) What’s the purpose of Pass-phrase key in PGP?

- Pass-phrase key is used to encrypt/decrypt the private keys of a user which are stored in the private-key ring.

6) How do PGP manage keys?

PGP uses key rings to manage keys:

One or more keys stored together constitute a key-ring. There are two classes:

- Private-key ring: Stores the private/public key pairs owned at this node.
- Public-key ring: Stores the public keys of other users known at this node.

7) Name the basic security requirements for email security.

- Confidentiality.
- Authentication.
- Integrity.

8) What are the differences between MIME and S/MIME?

- MIME is an extended framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) and RFC5322 or some other mail transfer protocol and emails.
- S/MIME is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

9) How does S/MIME process certificates?

- Uses public-key certificates that conform to X.509 v3.
- Key management is hybrid between X.509 and PGP’s web of trust.
- Each client has a list of trusted CA’s certificates and own public/private key pairs & certificates.
- Certificates must be signed by trusted CAs