Feedback on Topic 10 Ex

Exercise Question – E10.1

In secure email systems, such as PGP (pretty good privacy), the order of message protection operations performed by a sending entity is to first sign the outgoing/email message, then compress the signed message, and finally encrypt the compressed message. Answer the following questions:

(i) What are the justifications (or benefits) for using this order of operations, and

(ii) Would this order of operations be suitable for all cases of applications?

(iii) Assuming that Alice sends Bob an email, M. Express the whole message that is sent by Alice using protocol notation format.

Exercise Question – E10.1 - A

(i) Signature verification can only be carried out after two decryption operations and this makes the solution vulnerable to DoS attacks. However, as this is an end user to end user communication, so the issue of DoS attacks is considered not as important as users' preference of record-keeping a signed email (on plaintext). Compression-then-encryption can bring two benefits, one is security (harder to break a text that is not recognisible) and the other is performance (cheaper to encrypt a shorter message)

(ii) This order of operations is not suited to the cases where the operations are carried out by intermediary devices, as this would impact on the performance – reducing throughput and vulnerable to DoS attacks.

(iii) As shown in slide 12,

[ID of KUb]||E[KUb, Ks]||E[Ks, Compressed(TS||ID of KUa||2-bytesofSig||Sig(H[TS||M)||FileName||TS||Data]

Exercise Question – E10.2

Contrast the two trust models in terms of their respective merits and weaknesses:

- PKI X.509
- PGP web-of-trust

Exercise Question – E10.2 - A

PGP:

- the one significant advantage that PGP had, was that no certification infrastructure was needed before anyone could use PGP.
- Not scalable when a large number of users are involved.
- Certificates do not have a period of validity (they are infinitely valid), and their revocations are left to the user not by the CA.
- The certificate structure gives no indication of any authorization associated with key; again, this is left to the users.