Ne twork Security Technology	Spring, 2019
Tutorial 5, Week 6 (April 3)	LIU Zhen
Due Date: April 10	

Questions:

1. **Key Exchange** Consider the following protocol, where E is a symmetric key encryption scheme, and K is computed as $K = g^{ab}$.

$$\begin{array}{lcll} A & \rightarrow & B & : \text{ “I'm Alice”, } g^a \\ A & \leftarrow & B & : \text{ “Bob”, } g^b, E_K([g^a, g^b]_{\text{Bob}}) \\ A & \rightarrow & B & : \text{ “Alice”, } E_K([g^a, g^b]_{\text{Alice}}) \end{array}$$

   (a) What is the long-term secret of this scheme?

   (b) Does the protocol support forward secrecy?

   Solution

   (a) The long-term secret of this scheme are the private signing keys of Alice and Bob.

   (b) The protocol supports Perfect Forward Secrecy. The session keys are ephemeral Diffie-Hellman keys and the secrets will be discarded after each session. A compromise of the signing keys will therefore not affect the secrecy of previously agreed session keys.

2. **Authentication** Consider the following protocol, where E is a symmetric key encryption scheme and K is a long-term symmetric key shared between A and B.

$$\begin{array}{lcll} A & \rightarrow & B & : \text{ “Alice”, } R_1 \\ A & \leftarrow & B & : R_2, E_K(R_1) \\ A & \rightarrow & B & : E_K(R_2) \end{array}$$

   (a) Does the scheme support session key establishment? If not, modify the protocol so that it does.

   (b) Does your protocol proposed in (a) support Perfect Forward Secrecy? If not, modify it so it supports PFS without adding any new encryption, digital signature or additional message flows.

   Solution

   (a) The protocol does not support session key establishment, because all random numbers (R_1, R_2) are public. Neither of them can be used as a session key. We modify the protocol as follows:

$$\begin{array}{lcll} A & \rightarrow & B & : \text{ “Alice”, } R_1 \\ A & \leftarrow & B & : R_2, E_K(R_1, R_2, K') \\ A & \rightarrow & B & : E_K(R_2, K') \end{array}$$

   Bob chooses a random session key K', which is encrypted together with the R_1 and R_2 and sent to Alice. Because K' is encrypted, an eavesdropper cannot learn K'.

   (b) The scheme does not support PFS. If somehow K becomes known to an attacker, he can decrypt previously recorded $E_K(R_1, R_2, K')$ to obtain K'. The following modification prevents this problem:

$$
\begin{array}{lcll}
A & \rightarrow & B & : \quad \text{“Alice”}, \; g^a \\
A & \leftarrow & B & : \quad g^b, \; E_K(g^a, g^b) \\
A & \rightarrow & B & : \quad E_K(g^b)
\end{array}
$$

In this protocol the session key is computed as $K = g^{ab}$ and the secrets are discarded after each session. This protocol supports PFS.