Network Security Technology Spring, 2019
Tutorial 6, Week 7 (April 10) LIU Zhen
Due Date: April 17

Questions:

1. **SSL** Consider the SSL protocol shown below (with $K = h(S, R_A, R_B)$):

$$\begin{array}{llllll} 1. & A & \rightarrow & B & : & R_A \\ 2. & A & \leftarrow & B & : & \text{Cert}_B,\ R_B \\ 3. & A & \rightarrow & B & : & \{S\}_B, E(K, h(msgs \mid\mid K)) \\ 4. & A & \leftarrow & B & : & h(msgs \mid\mid K) \\ 5. & A & \leftrightarrow & B & : & \text{Data encrypted under } K \end{array}$$

   (a) In step 3, if we change $E(K, h(msgs \mid\mid K))$ to $h(msgs \mid\mid K)$, will the protocol still be secure?

   (b) What exactly is the purpose of the message $E(K, h(msgs \mid\mid K))$ sent in step 3?

   (c) If we remove this part in step 3, i.e., if we changed step 3 to

$$3. \quad A \quad \rightarrow \quad B \quad : \quad \{S\}_B$$

   Would the protocol still be secure?

2. **IKE (1)** In IKE Phase 1 digital-signature-based aggressive mode (see below), proof_A and proof_B are signed by Alice and Bob, respectively. However, in IKE Phase 1 public-key-encryption-based aggressive mode, proof_A and proof_B are neither signed nor encrypted. Explain why they can still securely perform the authentication.

$$\begin{array}{llllll} 1. & A & \rightarrow & B & : & \text{CP},\ g^a \bmod p,\ \{\text{“Alice”}\}_{\text{Bob}},\ \{R_A\}_{\text{Bob}} \\ 2. & A & \leftarrow & B & : & \text{CS},\ g^b \bmod p,\ \{\text{“Bob”}\}_{\text{Alice}},\ \{R_B\}_{\text{Alice}},\ \text{proof}_B \\ 3. & A & \rightarrow & B & : & \text{proof}_A \end{array}$$

$$\begin{aligned} \text{proof}_A &= h(\text{SKEYID}, g^a \bmod p, g^b \bmod p, CP, \text{“}Alice''\text{)} \\ \text{SKEYID} &= h(g^{ab} \bmod p, R_A, R_B) \end{aligned}$$

3. **IKE (2)** Imagine you have a key exchange protocol similar to main mode in IKE Phase 1, but adding an additional piece of data (“cookies”, C_A and C_B) to the message flow:

$$\begin{array}{llllll} 1. & A & \rightarrow & B & : & \text{CP},\ \text{C}_A \\ 2. & A & \leftarrow & B & : & \text{CS},\ \text{C}_A,\ \text{C}_B \\ 3. & A & \rightarrow & B & : & g^a \bmod p, R_A,\ \text{C}_A,\ \text{C}_B \\ 4. & A & \leftarrow & B & : & g^b \bmod p, R_B,\ \text{C}_A,\ \text{C}_B \\ 5. & A & \rightarrow & B & : & \text{E(K, “Alice” } \mid\mid \text{ proof}_A\text{)} \\ 6. & A & \leftarrow & B & : & \text{E(K, “Bob” } \mid\mid \text{ proof}_B\text{)} \\ 7. & A & \leftrightarrow & B & : & \text{Data encrypted under } K \end{array}$$

   The cookies are in the form

$$C_x = h(K_x, \text{IP}_{peer}, \text{timestamp})$$

   where K_x is a secret key only known to the party creating the cookie and IP_{peer} is the IP address of the peer (i.e., Alice would put Bob's IP and vice versa).

(a) What are the reasons for including such cookies in the exchange?

(b) The function of these cookies has to be effective before the exchange reaches step 5, otherwise B could be in trouble. Can you explain why?

4. **IKE (3)** IKE Phase 1 signature-based main mode has 6 moves, while the aggressive mode has 3 moves only.

   (a) Give two advantages of the main mode over the aggressive mode.

   (b) Give one disadvantage of the main mode over the aggressive mode.