Nwtwork Security Technology Spring, 2021
Tutorial 7, Week 7 (April 13) LIU Zhen
Due Date: April 20

Questions:

1. **SSL (50 points)** 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 (50 points)** 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.

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

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