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?

   Solution

   (a) Even if we change the encryption of the hash to simply the hash itself the protocol will still be secure. Only Bob can decrypt $\{S\}_B$ and generate the correct $h(msgs \mid\mid K)$, thus Alice can still be certain she is talking to Bob.

   (b) The message $E(K, h(msgs \mid\mid K))$ sent in step 3 can be used to make denial-of-service attacks harder. If this message is removed, an attacker can simply send a random number to Bob in step 3 and then abandoning the connection, forcing Bob to keep it open until it times out, wasting resources on Bob's side. If the attacker repeats this many times from different sources until a limit is reached, Bob will stop accepting new connections and the DoS attack is successful.
   If the message $E(K, h(msgs \mid\mid K))$ is included, the attacker has to launch a replay attack instead, making it harder as he has to eavesdrop on a legitimate connection first.

   (c) The protocol would still be secure, even without that message. It could be more vulnerable to denial-of-service attacks, though.

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.

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

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

Solution We can see that the proof is neither signed nor encrypted. Nevertheless, in step 1 and 2 of the exchange the values R_A and R_B are encrypted for the respective recipient. The proof contains SKEYID, which in turn requires the knowledge of both R_A and R_B, which are only known to Alice and Bob and cannot be determined by an attacker. Hence, an attacker will be unable to impersonate either of them, as it cannot calculate the correct proof.

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:

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

The cookies are in the form

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

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?

Solution

(a) These cookies can help identifying spoofed packets (i.e., packets containing a fake sender address). Imagine an attacker T is sending packets to B containing a sender address A, by first sending CP and C_A to B. B will respond with CS, C_A, C_B. But because the packets are spoofed, B will send them to the address of A and the attacker will in fact not receive C_B from B. When it then tries to send $g^a \bmod p, R_A$, C_A, C_B to B, B will in fact notice that the exchange was spoofed because the included C_B will be incorrect.

(b) As indicated in (a), the cookies help prevent spoofed exchanges, that means if the cookies are correct, B assumes that A is a legitimate user and that the exchange should go ahead. B has to be sure that this is the case, because steps 5 and 6 involve actually calculating K which requires an exponentiation ($g^{ab} \bmod p$). This is a quite expensive operation. If an attacker could generate thousands of spoofed exchanges and B would need to do an exponentiation for each exchange, the attacker could quickly exhaust the computational resources of B, effectively launching a denial-of-service attack.

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.

Solution

(a) Advantages:

- A and B can negotiate the system paramters such as g and p, there is no need to pre-share the parameters.
- Main mode protects the identity of the two entities involved in the exchange. An eavesdropper cannot learn the identities in the exchange.

(b) Disadvantage:

- Main mode obviously requires twice as many messages to complete.