Homework 6

Pan Yisheng
515021910384

April 20, 2018

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

$$A \to B\text{: } R_A$$

$$A \leftarrow B : Cert_B, R_B$$

$$A \to B : \{S\}_B, E(K, h(msgs||K))$$

$$A \leftarrow B : h(msgs||K)$$

$$A \longleftrightarrow B : \text{Data encrypted under } K$$

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

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

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

$$A \to B \quad : \quad \{S\}_B$$

Would the protocol still be secure?

Solution a): Yes, the protocol will still be secure. Attacker can't also recover *msgs* and K even if $h(msgs||K)$ is not encrypted.

b): The purpose is to convince $\{S\}_B$ is not modified. In other word, it verify that the key is indeed K.

c): The protocol won't be secure. The message can be sent from A or anyone else using B's public key

Problem 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-keyencryption-based aggressive mode, $proof_A$ and $proof_B$ are neither signed nor encrypted. Explain why they can still securely perform the authentication.

$$A \rightarrow B\text{: CP},g^a \bmod p,\{\text{"}Alice\text{"}\}_{Bob},\ \{R_A\}_{Bob}$$

$$A \leftarrow B\text{: CS},g^b \bmod p,\{\text{"}Bob\text{"}\}_{Alice},\{R_B\}_{Alice},proof_B$$

$$A \rightarrow B\text{: } proof_A$$

$$proof_A = h(SKEYID, g^a \bmod p, g^b \bmod p, CP, \text{"}Alice\text{"})$$

$$SKEYID = h(g^{ab} \bmod p, R_A, R_B)$$

Solution In the public-keyencryption-based aggressive mode, the ID "Alice" and "Bod" are encrypted with public key which has the similar effects like digital signature. The middle attacker can't get the identities of A and B, so he can't diaguise as A or B so that the attack will fail.

Problem 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:

$$A \rightarrow B\text{:CP},C_A$$

$$A \leftarrow B\text{:CS, } C_A,C_B$$

$$A \rightarrow B\text{: } g^a \bmod p,R_A,C_A,C_B$$

$$A \leftarrow B\text{: } g^b \bmod p,R_B,C_A,C_B$$

$$A \rightarrow B\text{: } h(K,\text{"}Alice\text{"}||proof_A)$$

$$A \leftarrow B\text{: } h(K,\text{"}Bob\text{"}||proof_B)$$

$$A \longleftrightarrow B\text{:Data encrypted under } K$$

The cookies are in the form

$$C_x = h(K_x, IP_{peer}, timestamp)$$

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 Bobs 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):

1. K_x avoids attacker generate fake cookies.
2. IP_{peer} avoids middle-in-the-middle cookies.
3. timestamp avoids replay attacks.

b):The cookies can avoid attacker pretend to be A or B in the key exchange period. Otherwise, key exchange may fail.

Problem 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):

- we can protect identities in main mode
- we can negotiate g and p

b):In symmetric key based main mode, Alice's ID must be IP address!