COMP90043 Cryptography and Security
Semester 2, 2021, Workshop Week 12 Solutions

Authentication

1. What are the steps involved in an authentication process?
   Two steps are involved in an authentication process.
   Identification step: Presenting an identifier to the security system.
   Verification step: Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

2. What is a suppress-replay attack?
   Give an example of attack when a party's clock is ahead of that of the KDC.
   Give an example of attack when a party's clock is ahead of that of another party.

   When a sender's clock is ahead of the intended recipient's clock, an opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient's site. This replay could cause unexpected results.

   An unintentionally post-dated message (message with a clock time that is in the future with respect to the recipient's clock) that requests a key is sent by a client. An adversary blocks this request message from reaching the KDC. The client gets no response and thinks that an omission or performance failure has occurred. Later, when the client is off-line, the adversary replays the suppressed message from the same workstation (with the same network address) and establishes a secure connection in the client's name.

   An unintentionally post-dated message that requests a stock purchase could be suppressed and replayed later, resulting in a stock purchase when the stock price had already changed significantly.

3. Consider Mutual Authentication proposed by Woo and Lam.

   (a) $A \rightarrow KDC : ID_A||ID_B$

   (b) $KDC \rightarrow A : E(PR_{auth}, [ID_B||PU_b])$

   (c) $A \rightarrow B : E(PU_b, [N_a||ID_A])$

   (d) $B \rightarrow KDC : ID_A||ID_B||E(PU_{auth}, N_a)$

   (e) $KDC \rightarrow B : E(PR_{auth}, [ID_A||PU_a])||E(PU_b, E(PR_{auth}, [N_a||K_s||ID_A||ID_B]))$

   (f) $B \rightarrow A : E(PU_a, [N_b||E(PR_{auth}, [N_a||K_s||ID_A||ID_B])])$

   (g) $A \rightarrow B : E(K_s, N_b)$

   The protocol can be reduced from 7 steps to 5. Show the message transmitted at each step. Hint: the final message in this protocol is the same as the final message in the original protocol.

(a) $A \rightarrow B : ID_A||N_a$

(b) $B \rightarrow KDC : ID_A||ID_B||N_a||N_b$

(c) $KDC \rightarrow B : E(PR_{auth}, [ID_A||PU_a])||E(PU_b, E(PR_{auth}, [N_a||N_b||K_s||ID_A||ID_B]))$

(d) $B \rightarrow A : E(PU_a, E(PR_{auth}, [N_a||N_b||K_s||ID_A||ID_B]))$

(e) $A \rightarrow B : E(K_s, N_b)$

4. (a) List three general approaches to deal with replay attacks.

   i. Attach a sequence number to each message used in an authentication exchange. A new message is accepted only if its sequence number is in the proper order.

   ii. Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgement, is close enough to A's knowledge of current time. This approach requires that clocks among the various participants be synchronized.

   iii. Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

   (b) List three typical ways to use nonce as challenge.
   Suppose N_a is a nonce generated by A, A and B share key K, and $f()$ is a function (such as an increment).

   i. $A \rightarrow B : N_a$
   $B \rightarrow A : E(K, N_a)$

   ii. $A \rightarrow B : E(K, N_a)$
   $B \rightarrow A : N_a$

   iii. $A \rightarrow B : E(K, N_a)$
   $B \rightarrow A : E(K, f(N_a))$

Merkle trees

5. Evaluation the proof size of an n-ary tree. Show that binary is minimal. The proof size is proportional to the number of neighbours at each node.