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

Authentication

1. What are the steps involved in an authentication process?

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.

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) $A \rightarrow B :$

   (b) $B \rightarrow KDC :$

   (c) $KDC \rightarrow B :$

   (d) $B \rightarrow A :$

   (e) $A \rightarrow B :$

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

   (b) List three typical ways to use nonce as challenge.

Merkle trees

5. Evaluation the proof size of an n-ary tree. Show that binary is minimal.