FIT3031-Tutorial 4

AUTHENTICATION APPLICATIONS

Q1 What problem was Kerberos designed to address?

Q2 What are the three threats associated with user authentication over a network or Internet?

Q3 List three approaches to secure user authentication in a distributed environment.

Q4 What four requirements were defined for Kerberos?

Q5 What are the essential ingredients of a public-key directory?

Q6 What are the requirements for the use of a public-key certificate scheme?

Q7 What is the purpose of the X.509 standard?

Q8 What is a chain of certificates?

Q9 How is an X.509 certificate revoked?

Problems:

1. There are 3 typical ways to use nonces as challenges. Suppose N_a is a nonce generated by A, A and B share key K, and f() is a function (such as increment). The three usages are:

Usage 1	**Usage 2**	**Usage 3**
(1) A → B: N_a (2) B → A:E(K, N_a)	(1) A → B: E(K, N_a) (2) B → A: N_a	(1) A → B: E(K, N_a) (2) B → A: E(K, f(N_a))

Describe situations for which each usage is appropriate.

2. Consider a one-way authentication technique based on asymmetric encryption:

   A → B: ID_A
   B → A: R_1
   A → B: E(PR_a, R_1)

   a. Explain the protocol.
   b. What type of attacks is this protocol susceptible to?

3. In Kerberos, when Bob receives a ticket from Alice, how does he know it is genuine?

4. In Kerberos, Alice receives a reply, how does she know it came from Bob (that it's not a replay of an earlier message from Bob)?

5. Consider the following protocol:

   A → KDC: $ID_A \parallel ID_B \parallel N_1$
   KDC → A: $E(K_a,[K_S \parallel ID_B \parallel N_1 \parallel E(K_b,[K_S \parallel ID_A]))$
   A → B: $E(K_b,[K_S \parallel ID_A])$
   B → A: $E(K_S, N_2)$
   A → B: $E(K_S, f(N_2))$

   a. Explain the protocol
   b. Can you think of a possible attack on this protocol, if an old key, K_S is compromised? Explain how it can be done.
   c. Mention a possible technique to get around the attack — not a detailed mechanism, just the basics of the idea.

6. Explain the problems with key management and how it affects symmetric cryptography?