COMP00043: Cryptography and Security

Week 11 WorkshopActivity

Before we begin, take a few minutes to discuss the following:

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

1. List three general approaches to dealing with replay attacks.

2. What is a suppress-replay attack?

Now try the following questions:

1. Consider Mutual Authentication proposed by Woo and Lam in Section 15.4. The protocol referred presented there can be reduced from seven steps to five, having the following sequence:

   (a) $A \to B$:

   (b) $B \to KDC$:

   (c) $KDC \to B$:

   (d) $B \to A$:

   (e) $A \to B$:

   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.

2. Reference the suppress-replay attack described in Section 15.2 to answer the following.

   (a) Give an example of an attack when a party's clock is ahead of that of the KDC.

   (b) Give an example of an attack when a party's clock is ahead of that of another party.

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

Usage 1	**Usage 2**	**Usage 3**
(1) $A \to B : N_a$	(1) $A \to B : E(K, N_a)$	(1) $A \to B : E(K, N_a)$
(2) $B \to A : E(K, N_a)$	(2) $B \to A : N_a$	(2) $B \to A : E(K, f(N_a))$

   Describe situations for which each usage is appropriate.

Home Work:

1. In addition to providing a standard for public-key certificate formats, X.509 specifies an authentication protocol. The original version of X.509 contains a security flaw. The essence of the protocol is as follows:

$$A \rightarrow B : At_A, r_A, ID_B$$

$$B \rightarrow A : Bt_B, r_B, ID_A, r_A$$

$$A \rightarrow B : Ar_B$$

Where t_A and t_B are timestamps, r_A and r_B are nonces and the notation X{Y} indicates that the message Y is transmitted, encrypted, and signed by X.

The text of X.509 states that checking timestamps t_A and t_B is optional for three-way authentication. But consider the following example: Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B:

$$C \rightarrow B : A0, r_A, ID_B$$

B responds, thinking it is talking to A but is actually talking to C:

$B \rightarrow C : B0, r‘_B, ID_A, r_A$

C meanwhile causes A to initiate authentication with C by some means. As a result, A sends C the following:

$A \rightarrow C : A0, r‘_A, ID_C$

C responds to A using the same nonce provided to C by B:

$C \rightarrow A : C0, r´_B, ID_A, r‘_A$

A responds with

$A \rightarrow C : Ar‘_B$

This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B.

$C \rightarrow B : Ar‘_B$

So B will believe it is talking to A whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps.