Internet Infrastructure Security (COMP444)

A5

Due at 11:55pm on 26 March 2015

Submission site: `https://submit.comp.polyu.edu.hk/`

Rocky K. C. Chang

March 12, 2015

1. `[6 marks]` (Diffie-Hellman protocol) Consider that Alice and Bob are conducting Diffie-Hellman protocol to come up a secret key. They agree to use $p = 19$ and $g = 2$.
   (a) `[2 marks]` If Alice picks $x = 2$, what is the set of secret keys that can be generated?
   (b) `[2 marks]` If Bob picks $y = 3$, what is the set of secret keys that can be generated?
   (c) `[2 marks]` Based on (a) and (b), what are the possible final secret keys?

2. `[6 marks]` (A slightly different DH protocol) Another Diffie-Hellman protocol variant is to allow one side to completely determine the shared key. The first few steps are depicted as follows. What should Bob do in the last step in order to derive the same key chosen by Alice?
   (a) Alice randomly selects a large integer x and compute $k = g^x \ mod \ p$.
   (b) Bob randomly selects a large integer y and sends Alice $Y = g^y \ mod \ p$.
   (c) Alice sends Bob $X = Y^x \ mod \ p$.
   (d) Bob ?

3. `[6 marks]` (Attacking the Diffie-Hellman exchange) In this question we consider an active attack on the Diffie-Hellman exchange. Before Eve launches this attack, she has to understand certain elementary properties about the multiplicative group modulo prime. In the last question, we have already proved that 1 and $p - 1$ are the only elements in $\mathbb{Z}_p^*$ that their multiplicative inverses are themselves.
   (a) `[3 marks]` Consider that p is a safe prime. That is, $p = 2q + 1$, where q is prime, and g is a generator for $\mathbb{Z}_p^*$. Show that $g^q \equiv p - 1 (\mathrm{mod}\ p)$. You may start with the property that $g^{p-1} \bmod p = 1$.
   (b) `[3 marks]` Now consider the attack. Alice and Bob exchange $g^x \bmod p$ and $g^y \bmod p$. Eve intercepts the messages and changes them to $(g^x)^q \bmod p$ and $(g^y)^q \bmod p$, respectively. What is the result of this attack?

4. `[6 marks]` (Mutual authentication) Consider the following mutual authentication protocol where A and B conduct a Diffie-Hellman protocol to come up $K_{AB} = g^{xy} \mod p$. A and B have agreed on a multiplicative group $\mathbb{Z}_p^*$, and they pick their random numbers x and y from $\mathbb{Z}_p^*$, respectively. Assume that each side can authenticate the other based on digital signatures, and $Sig_A()$ and $Sig_B()$ denote A's and B's signatures, respectively. The signatures are also encrypted by K_{AB}.

1. $A \rightarrow B : A, B, g^x \mod p$

2. $B \rightarrow A : B, A, g^y \mod p, \{Sig_B(g^y \mod p, g^x \mod p)\}_{K_{AB}}$

3. $A \rightarrow B : A, B, \{Sig_A(g^x \mod p, g^y \mod p)\}_{K_{AB}}$

Unfortunately, this protocol is also vulnerable to impersonation attack. Consider that A's first protocol message sent to B is intercepted by an attacker C, and subsequently C could complete the protocol with A successfully. The notation C_B refers to C claiming to be B. Fill in the missing steps below.

1. $A \rightarrow C_B : A, B, g^x \mod p$

1'. $C \rightarrow B :$?

2'. $B \rightarrow C :$?

2. $C_B \rightarrow A : B, A, g^y \mod p, \{Sig_B(g^y \mod p, g^x \mod p)\}_{K_{AB}}$

3. $A \rightarrow C_B : A, B, \{Sig_A(g^x \mod p, g^y \mod p)\}_{K_{AB}}$

5. `[6 marks]` (Authenticated key exchange) Consider the following authenticated key exchange protocol between A and B. Assume that each side can authenticate the other based on digital signatures, and $Sig_A()$ and $Sig_B()$ denote A's and B's signatures, respectively. In step 1, A generates a pair of RSA private and public keys, and sends the public key K_p to B. $E_{K_p}()$ is encryption using the public key K_p, K_{AB} is the session key chosen by B, and N_A is A's nonce.

1. $A \rightarrow B : K_p, N_A, Sig_A(K_p, B)$

2. $B \rightarrow A : E_{K_p}(K_{AB}), Sig_B(h(K_{AB}), A, N_A)$

   (a) `[2 marks]` What is the purpose of generating a pair of RSA keys in step 1?

   (b) `[2 marks]` What is the purpose of using a hash function $h()$ in step 2?

   (c) `[2 marks]` As soon as A receives the message from B, A will destroy the RSA key pair. In this case, will this protocol achieve forward perfect secrecy if A's or B's key for signing is known to an attacker?

6. `[6 marks]` (One-way authentication) Consider the following protocol for A to authenticate B using public-key signature. N_A is a nonce selected by A, and $SIG_B(N_A)$ is B's signature over N_A.

(1) $A \rightarrow B : N_A$

(2) $B \rightarrow A : SIG_B(N_A)$

Like many other protocols that you have seen before, this one suffers from an impersonation attack. Consider that C impersonates B by creating two sessions: one with A and the other with B. Fill in the missing messages below and explain your answer. The notation C_B refers to C claiming to be B.

(1) $A \rightarrow C_B : \ N_A$

(1') $C \rightarrow B :$?

(2') $B \rightarrow C :$?

(2) $C_B \rightarrow A :$?