SICUREZZA NELLE RETI
Laurea Specialistica in Ingegneria Informatica

SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)
Laurea Magistrale in Ingegneria Informatica

SECURITY IN NETWORKED COMPUTING SYSTEMS
Computer Engineering

20 February 2017

NAME ____ SERIAL NO. ______________________

EXERCISE NO. 1 (LMCE, LMECS) #MARKS: 12

1. Introduce the Diffie-Hellman key exchange scheme.
2. Argue about its security w.r.t. a passive adversary.
3. Argue about its vulnerability to the main-in-the-middle attack and propose a solution.

EXERCISE NO. 2 (LMCE) #MARKS: 10

Let us consider the modified version of the Diffie-Hellman protocol reported below and aimed at establishing a session key K_{AB}, $K_{AB} = g^{x_A x_B} mod\ p$, between user Alice and server Bob, with P a secret password shared between Alice and Bob.

$$M1\ A \rightarrow B: \quad A, \{g^{x_A} mod\ p\}_P$$
$$M2\ B \rightarrow A: \quad B, \{g^{x_B} mod\ p\}_P$$

1) Which of these are drawbacks of using the protocol (argue the answer)?
   a) It is vulnerable to offline password-dictionary attacks.
   b) It requires server Bob to store passwords in the clear-text.
   c) It is vulnerable to the *man-in-the-middle* attack.

(2) Does the protocol guarantees identification, i.e., A knows that B is present and/or vice versa (argue the answer)?
   A. No;
   B. Yes, A w.r.t. B;
   C. Yes, B w.r.t. A;
   D. Yes, both.

(3) Extend the protocol in order to achieve mutual authentication.

EXERCISE NO. 3 (LMCE, LMECS) #marks: 8

Let K_A be the public key of Alice, $S_P(x)$ be the digital signature of principal P on item x, CA be a Certification Authority (trusted by all principals of the system), and finally H a secure hash function. Which of the following certificates are useful to establish a secure channel with Alice (do not consider the validity interval)? Argue why.

(A) "Alice" || S_{CA}(H("Alice"|| K_A))
(B) "Alice" || K_A || S_A("Alice" || K_A)
(C) "Alice" || K_A || S_{CA}("Alice" || H(K_A))
(D) "Alice" || K_A || S_{CA}(H("Alice" || K_A))
(E) "Alice" || K_A || S_{CA} (K_A)
(F) "Alice" || K_A || S_B("Alice" || H(K_A) || "issuer: Bob") || S_{CA}("Bob" || K_B)
(G) "Alice" || K_A || S_B("Alice" || H(KA) || "issuer: Bob") || SCA("Bob, CA=Yes" || KB)

20 February 2017

SOLUTION

EXERCISE #1

See theory.

EXERCISE #2.

Question (1)

A. The protocol is not subject to an offline dictionary attack because the plaintext of M1 is a random number.
B. The protocol requires a server to store a password in clear-text.
C. The protocol is not vulnerable to a MIM because the adversary does not know the password *P*.

Question (2)

The protocol does not guarantee identification because A does has not received any fresh material encrypted by K_{AB} at the end of the protocol, and vice versa.

Question (3)

M1 $A \rightarrow B: \; n_A$

M2 $B \rightarrow A: \; \{n_B, n_A, g^{x_B} \bmod p\}_P$

M3 $A \rightarrow B: \; \{n_B, g^{x_A} \bmod p\}_{K_{AB}}$

M4 $B \rightarrow A: \; \{n_B, n_A\}_{K_{AB}}$

EXERCISE #3.

(A) It is not good because there is no way to extract Alice's public key from the certificate.
(B) It is not good because it is a self-certified certificate.
(C) Good
(D) Good
(E) It is not good because it does not link Alice's identifier "Alice" to Alice's public key K_A.
(F) It is not good, because the Certification Authority CA (root of trust) has not delegated Bob to serve as a Certification Authority
(G) Good. It describes a case of certificate chain where Bob has been properly delegated by the Certification Authority CA to serve as a sub-CA.