Homework 11 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

17.01.2012

Exercise 32. We consider an authenticated shared-key key-agreement protocol, also known as the *Needham-Schroeder* protocol. K_{TA} is the shared key between the trusted server T and A. K_{TB} is the shared key between T and B. K_S is a shared session key created by T. r_A, r_B are random numbers generated by A, B.

Protocol actions

(1) : $A \to T : A, B, r_A$

(2) : $T \to A : E_{K_{TA}}(r_A, B, K_S, E_{K_{TB}}(K_S, A))$

(3) : $A \to B : E_{K_{TB}}(K_S, A)$

(4) : $B \to A : E_{K_S}(r_B)$

(5) : $A \to B : E_{K_S}(r_B - 1)$

(a) Attack the system assuming Oscar O knows a key K'_S and its ticket $E_{K_{TB}}(K'_S, A)$.

(b) Assume, B can not store older shared keys. Prevent the attack of (a). You may include an encrypted authenticator $a = E_{K_{TB}}(A, t_b)$ issued by B to A with a secret time stamp t_b.

Now, we consider an authenticated public-key key-agreement protocol. P_A, P_B are public keys of A and B. S_T is a signature by T and cert_T the authentic public signature key. r_A, r_B are random numbers generated by A and B. Users must retrieve public keys from T.

Protocol actions

(1) : $A \to T : A, B$

(2) : $T \to A : \text{cert}_T, S_T(P_B, B)$

(3) : $A \to B : E_{P_B}(r_A, A)$

(4) : $B \to T : B, A$

(5) : $T \to B : \text{cert}_T, S_T(P_A, A)$

(6) : $B \to A : E_{P_A}(r_A, r_B)$

(7) : $A \to B : E_{P_B}(r_B)$

(c) Show that this protocol is vulnerable to a man-in-the-middle attack.

(d) Prevent the attack of (c). You may include an identifier.

Exercise 33.

The following challenge-response protocol based on digital signatures is given:

(1) $A \leftarrow B : r_B$

(2) $A \rightarrow B : r_A, S_A(r_A, r_B, B)$

(3) $A \leftarrow B : r'_B, S_B(r'_B, r_A, A)$

(a) Explain how Oscar O can authenticate to A without signing any message with his own identity. This is called an interleaving attack.