Musterlösung <u>Cryptography II Übung 11</u> 17.1.12

eher nicht Klausurrelevant

Exercise 32

Given: • shared keys K_{TA}, K_{TB}, K_S
• random numbers r_A, r_B
• a broken K_S' and its ticket $E_{KTB}(K_S', A)$
both known to Oscar

a) authentication attack:

older session

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

$(2)\ T \to A : E_{KTA}(r_A, B, K_S', \overbrace{E_{KTB}(K_S', A)}^{\text{ticket}})$

$(3)\ A \to O(B) : E_{KTB}(K_S', A)$ // O knows the key K_S' by assumption

$(4)\ O(A) \to B : E_{KTB}(K_S', A)$ // O forwards the old ticket that belongs to K_S'

$(5)\ B \to O(A) : E_{KS'}(r_B)$ // B uses the shared key

$(6)\ O(A) \to B : E_{KTB}(r_B - 1)$ // O knows the shared key

$\Rightarrow$ O is authenticated as A to B

b) $(1)\ A \to B : A$ // A asks B for an authenticator

$(2)\ B \to A : a = E_{KTB}(A, t_B)$

$(3)\ A \to T : A, B, r_A, a$ // A appends authenticator a

$(4)\ T \to A : \underbrace{E_{KTA}(r_A, B}, K_S, \underbrace{E_{KTB}(K_S, A, t_B)}_{\text{ticket}})$

$(5)\ A \to B : E_{KTB}(K_S, A, t_B)$

$(6)\ B \to A : E_{KS}(r_B)$ // B can check t_B

$(7)\ A \to B : E_{K_S}(r_B - 1)$ $\Rightarrow$ O can not forward an old ticket since he does not know the current t_B

c) Man-in-the-middle attack

- Assume there is a session between A and O

$(1)\ A \to T : A, O$ } A retrieves the public key P_O

$(2)\ T \to A : cert_T, S_T(P_O, O)$

$(3)\ A \to O : E_{P_O}(r_A, A)$

$(4)\ O \to T : O, B$ } O retrieves the public key P_B

$(5)\ T \to O : cert_T, S_T(P_B, B)$

...

$(6)\ O(A) \to B : E_{P_B}(r_A, A)$

$(7)\ B \to T : B, A$ } B retrieves public key P_A

$(8)\ T \to B : cert_T, S_T(P_A, A)$

$(9)\ B \to O(A) : E_{P_A}(r_A, r_B)$

$(10)\ O \to A : E_{P_A}(r_A, r_B)$ // O forwards (9)

$(11)\ A \to O : E_{P_O}(r_B)$ // O can use r_B

$(12)\ O(A) \to B : E_{P_B}(r_B - 1)$ // O is authenticated as A to B

Musterlösung   Cryptography II Übung 11   17.1.12

d) include identifier B at (6):

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

in attack: (9) $B \to O(A)$: $E_{P_A}(r_A, r_B, B)$
(10) $O \to A$: $E_{P_A}(r_A, r_B, B)$

$E_{P_A}(r_A, r_B', O)$

and O does not know $r_B' = r_B$

, but A expects to get $E_{P_A}(r_A, r_B, O)$ and O can only generate $E_{P_A}(r_A, r_B', O)$

Exercise 33

Interleaving attack

An interleaving attack uses information of simultaneous sessions combined

(1) $O(B) \to A$: r_B
(2) $A \to O(B)$: r_A, $S_A(r_A, r_B, B)$
(3) $O(A) \to B$: r_A
(4) $B \to O(A)$: r_B', $S_B(r_B', r_A, A)$
(5) $O(B) \to A$: r_B', $S_B(r_B', r_A, A)$