Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 22 luglio 2011

Nome e Cognome _____ **Matricola** _____

ESERCIZIO 1 — punti: 10

Il candidato presenti le proprietà di una funzione hash sicura (MDC) illustrandone la relazione con la firma digitale.

ESERCIZIO 2 — punti: 10

Si progetti un protocollo di distribuzione delle chiavi che permette ad Alice e Bob di stabilire una chiave di sessione K_{ab} attraverso Trent, un Key Destribution Center fidato. Alice e Bob non condividono *a-priori* alcun segreto a lungo termine. Al contrario, entrambi conoscono Π_T la chiave pubblica di Trent. Inoltre ciascuno di essi condivide con Trent un segreto che però non può essere utilizzato come chiave crittografica. Sia, ad esempio, π_A il segreto che Alice condivide con Trent. Si assuma che i clock siano sincronizzati.

Al termine di un'esecuzione, il protocollo deve garantire che i) Alice (Bob) conosca la chiave di sessione; ii) Alice (Bob) sappia che Bob (Alice) conosce la chiave di sessione; iii) attacchi di reply non siano possibili.

Il candidato è libero di scegliere lo schema di comunicazione.

ESERCIZIO 3 — punti: 10

Il candidato descriva il protocollo base di Kerberos discutendo il dimensionamento delle finestre temporali caratteristiche del protocollo.

Soluzione

ESERCIZIO 1

Vedi appunti.

ESERCIZIO 2

Ipotesi

1. $\forall P \in \{A, B\}, P \mid\equiv \overset{\Pi_T}{\mapsto} T$
2. $\forall P \in \{A, B\}, P \mid\equiv P \overset{\pi_p}{\rightleftharpoons} T, T \mid\equiv P \overset{\pi_p}{\rightleftharpoons} T$
3. $\forall P \in \{A, B\}, P \mid\equiv P \overset{K_p}{\leftrightarrow} T$
4. $\forall P \in \{A, B\}, T \mid\equiv \left(A \overset{K_{ab}}{\leftrightarrow} B \right)$
5. $\forall P \in \{A, B\}, P \mid\equiv T \Rightarrow \left(A \overset{K_{ab}}{\leftrightarrow} B \right)$
6. $\forall P \in \{A, B\}, T \mid\equiv P \Rightarrow \left(P \overset{K_p}{\leftrightarrow} T \right)$
7. $\forall P, Q \in \{A, B, T\}, P \mid\equiv \#\left(t_q\right)$

Protocollo idealizzato

M 1 $\quad A \rightarrow B: \quad \left\{ \left\langle A, B, \tau_a, A \overset{K_a}{\leftrightarrow} T \right\rangle_{\pi_a} \right\}_{\Pi_T}$

M 2 $\quad B \rightarrow T: \quad \left\{ \left\langle A, B, \tau_a, A \overset{K_a}{\leftrightarrow} T \right\rangle_{\pi_a} \right\}_{\Pi_T}, \left\{ \left\langle B, A, \tau_b, B \overset{K_b}{\leftrightarrow} T \right\rangle_{\pi_b} \right\}_{\Pi_T}$

M 3 $\quad T \rightarrow B: \quad \left\{ B, A, \tau_b + 1, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_b}, \left\{ A, B, \tau_a + 1, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_a}$

M 4 $\quad B \rightarrow A: \quad \left\{ A, B, \tau_a + 1, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_a}, \left\{ A, B, \tau_b', A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}}$

M 5 $\quad A \rightarrow B: \quad \left\{ B, A, \tau_b' + 1, A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{ab}}$

Protocollo reale

M 1 $A \rightarrow B : \quad A, B, \{A, B, \tau_a, K_a, \pi_a\}_{\Pi_T}$

M 2 $B \rightarrow T : \quad \{A, B, \tau_a, K_a, \pi_a\}_{\Pi_T}, \{B, A, \tau_b, K_b, \pi_b\}_{\Pi_T}$

M 3 $T \rightarrow B : \quad \{B, A, \tau_b, K_{ab}\}_{K_b}, \{A, B, \tau_a, K_{ab}\}_{K_a}$

M 4 $B \rightarrow A : \quad \{A, B, \tau_a, K_{ab}\}_{K_a}, \{A, B, \tau'_b\}_{K_{ab}}$

M 5 $A \rightarrow B : \quad \{B, A, \tau'_b\}_{K_{ab}}$

ESERCIZIO 3

Vedi appunti.