Laurea Specialistica in Ingegneria Informatica

SICUREZZA NELLE RETI

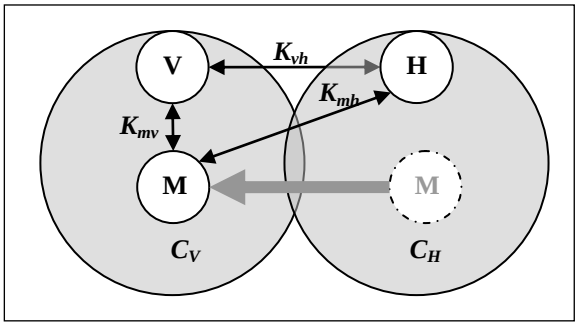
Appello del 24 luglio 2009

Esercizio 1 — punti: 10

Con proprietà di linguaggio e precisione matematica si discuta la sicurezza dell'algoritmo RSA.

Esercizio 2 — punti: 12

Si consideri il sistema semplificato di *roaming* riportato in figura in cui una stazione mobile *M* registrata presso l'*home server H* si trova nella cella C_V gestita dal server *visited server V*. Per garantire la comunicazione sicura della stazione mobile *M* è necessario che questa stabilisca un canale sicuro (la chiave simmetrica K_{vm}) con il visited server *V*. A tale proposito si assuma che:



A. in virtù della registrazione, la stazione mobile *M* ed l'home server *H* condividono la chiave k_{mh}.
B. i server *H* e *V* fanno parte dell'infrastruttura e pertanto condividono la chiave k_{vh};
C. la stazione mobile *M* ed i server *H*, *V* utilizzano lo stesso cifrario; ed infine
D. i loro clock non sono sincronizzati.

Progettare un protocollo di distribuzione delle chiavi che soddisfi i seguenti requisiti:

1. permette l'autenticazione mutua di *M* e *V* quando *M* entra nella cella C_V;
2. permette di distribuire una chiave di sessione k_{mv} tra *M* e *V*;
3. fornisce la prova a *V* che *M* possiede k_{mv} e viceversa;
4. mantiene la segretezza della chiave k_{mh};
5. è resistente ad attacchi di replay.

Il candidato argomenti per mezzo della logica BAN che il protocollo proposto soddisfa i requisiti posti.

Esercizio 3 — punti: 8

Si descrivano le informazioni minime che devono essere contenute in un certificato digitale ed i principali obblighi che un'autorità di certificazione deve assolvere per il rilascio di tale certificato.

Soluzione

Risposta a. Il protocollo garantisce la confidenzialità. Per determinare il valore di K_{AB} è necessario conoscere le quantità k_a e k_b. Tuttavia queste quantità viaggiano in rete in forma cifrata.

Risposta b. Il protocollo è una versione semplificata del protocollo Needham-Schroeder a chiave pubblica. Il protocollo garantisce la *key autentication*. Formalmente: $A \mid\equiv B \mid\equiv A \overset{k_b}{\mapsto} B$ **e** $B \mid\equiv A \mid\equiv A \overset{k_a}{\mapsto} B$ **.**

Risposta c. Come si evince dalle formule sopra, il protocollo garantisce anche la key confirmation.

Risposta d. Se l'ipotesi (i) non è verificata, il protocollo non garantisce la proprietà di key authentication. Supponiamo che la quantità k_a sia riutilizzata da *A* e che un avversario *M* abbia registrato i messaggi M1 ed M2 relativi all'esecuzione del protocollo in cui k_a è stata utilizzata la prima volta. L'avversario *M* potrebbe eseguire il seguente attacco:

- induce *A* ad iniziare una nuova istanza del protocollo con B;
- quando *A* invia il messaggio M1' relativo alla nuova esecuzione del protocollo, contenente la quantità riutilizzata k_a, l'avversario *M* determina che M1=M1', e risponde con M2. Alla ricezione di questo messaggio il processo A crede di parlare effettivamente con *B.*

Si noti che questo attacco ha come effetto collaterale il riutilizzo della vecchia chiave di sessione K_{ab} (la quantità k_b è contenuta nel messaggio M2 replicato da *M*). L'avversario *M* potrebbe non conoscere tale chiave ma potrebbe comunque replicare vecchi messaggi relativi alla sessione K_{ab} che *A* considererebbe come provenienti da *B*. Il danno sarebbe massimo se *M*, per altre vie, fosse riuscito ad impadronirsi di K_{ab}.

Considerazioni simili possono essere fatte per *B* se questo processo riutilizza la quantità k_b.