Prova scritta del 10 gennaio 2007 (5 punti)

Testo

Sia *PK* la *chiave pubblica* del server S e sia PIN un *segreto condiviso* tra il server S ed il cliente C. Si definisca un protocollo di distribuzione delle chiavi che, al termine della sua esecuzione, soddisfi i seguenti requisiti:

1. il cliente ed il server condividono una *chiave segreta di sessione K*;
2. il cliente ha identificato il server ed ha la prova che il server possiede la chiave *K*;
3. il server ha identificato il cliente ed ha la prova che il cliente possiede la chiave *K*;
4. il protocollo è resistente ad attacchi di *replay*.

Tali requisiti devo essere soddisfatti in presenza del seguente vincolo: per quanto riguarda la crittografia a chiave pubblica, il server ed il cliente dispongono solo di un cifrario (in altre parole la firma digitale non è disponibile).

Soluzione

Un protocollo che soddisfa i requisiti è il seguente

M1 $S \rightarrow C$: S, C, n
M2 $C \rightarrow S$: $C, S, E_{PK}(C, S, PIN, K, n)$
M3 $S \rightarrow C$: $S, C, E_K(S, C, n)$;

La chiave è un segreto condiviso tra cliente e server perchè in rete essa appare sempre nella sua forma cifrata.

Il cliente identifica il server alla ricezione del messaggio M3 perchè tale messaggio è cifrato con la chiave K. Siccome questa chiave è stata trasmessa nel messaggio M2 in forma cifrata per mezzo della chiave pubblica del server PK, allora solo il server può aver decifrato il messaggio M2 e originato il messaggio M3. Il server dà perciò prova al cliente di possedere la chiave K cifrando il messaggio M3 con tale chiave.

Dalla presenza del PIN nel messaggio M2, il server deduce che il mittente è il cliente e che questo possiede la chiave K.

Se *n* è una quantità "fresca", allora il server ha la possibilità di determinare se M2 è un replay oppure no. Se la chiave *K* è fresca (come deve essere una chiave di sessione), il cliente ha la possibilità di determinare se M3 è un replay oppure no.

Commento. L'utilizzo del PIN come chiave di cifratura non è da considerarsi una idea valida perchè non si riesce a fornire un adeguato compromesso tra sicurezza ed usabilità. Un PIN deve essere facilmente ricordabile da un umano, quindi avrà "pochi bit" e quindi non sarà una "buona" chiave. Un PIN usabile come chiave avrà "troppi" bit per poter essere "facilmente" ricordato da un umano.