Sicurezza nelle reti e nei sistemi informatici, esame del 26-1-2012
tempo: 120 minuti
NB: le domande non hanno necessariamente lo stesso peso

1 Confidenzialità ed integrità

a. Spiegare i termini *confidenzialità* ed *integrità*.
b. Alice e Bob hanno una coppia di chiavi pubblica/privata (PKA, SKA) e (PKB, SKB) ciascuno. Assumere che Alice conosca la chiave pubblica di Bob e che Bob conosca la chiave pubblica di Alice. Usiamo la notazione EncK(m) per la cifratura di m con la chiave K, SignK(m) per la firma di m con la chiave K e H(m) per lo hash sicuro di m. Alice vuole inviare alcuni file di grandi dimensioni a Bob su una rete pubblica, così da garantire confidenzialità ed integrità.

(b1) Supponiamo che, per ciascun file f, Alice invii a Bob il messaggio: EncPKB(f, SignSKA(H(f))). Spiegare brevemente se questo garantisce confidenzialità ed integrità. È una soluzione efficiente nel caso di dispositivi mobili con potere computazionale limitato?

(b2) Supponiamo ora che Alice e Bob vogliano usare una chiave simmetrica di sessione KAB per cifrare i file. Essi debbono dapprima concordare tale chiave. Supponiamo che il protocollo preveda che Bob sceglie la chiave KAB ed invia ad Alice il messaggio EncPKA(KAB). Quindi, per ciascun file f, Alice invia a Bob il messaggio EncKAB(f). Questo protocollo garantisce confidenzialità e integrità? Che vantaggi/svantaggi presenta rispetto al protocolla presentato in (b1)?

2 Diffie-Hellman

a) Discutere i maggiori punti di forza e di debolezza del protocollo Diffie-Hellman per definire una chiave segreta.
b) Discutere una soluzione che risolva le debolezze del protocollo.

3. Autenticazione

a) Mostrare un protocollo che usi un *nonce* per la mutua autenticazione fra due utenti che condividono una password segreta.
b) Mostrare un protocollo che usi un *nonce* per la mutua autenticazione fra due utenti che hanno una chiave pubblica.
c) Mostrare un protocollo basato su timestamp per la mutua autenticazione fra due utenti che condividono una chiave con un server centrale sicuro (come in kerberos).

4 Firewall

a) Discutere le principali differenze fra il filtraggio dei pacchetti *stateless* e *stateful* (cinque righe).

b) Disegnare uno schema che illustri come posizionare un firewall basato su filtraggio pacchetti nel caso di una piccola organizzazione che ha un server Web e un mail server accessibili dall'esterno/interno e una rete locale, con una base dati, che serve i dipendenti dell'organizzazione e quindi accessibile solo dall'interno.

c) Mostrare tramite un qualunque linguaggio/formalismo scelto a piacere come configurare il firewall dell'organizzazione in modo da consentire verso l'esterno solo connessioni Web (porta 80) e connessioni FTP (si rammenta che FTP usa la porta 21 per controllare la sessione e la porta 20 per scambiare dati). **NB: i servizi ipotizzati sono diversi da quelli descritti al punto b.**

5 Sicurezza delle applicazioni

a. Spiegare brevemente quali sono gli aspetti fondamentali di questo tipo di sicurezza (10 righe).
b. Illustrare il meccanismo dei *cookie* nei browser, spiegando quali sono gli usi impropri e i rischi corsi dall'utente. Spiegare come prevenire tali rischi.