Sicurezza nelle reti e nei sistemi informatici – 16/6/2011
Tempo: 100 minuti. N.B.: le domande potrebbero avere pesi differenti!

1. Integrità dei dati

a. Descrivere il concetto di *integrità dei dati* e come l'uso di una opportuna funzione di hashing possa aiutare a garantire tale requisito; discutere anche i limiti dell'approccio illustrato.
b. Alice deve inviare a Bob un file di M byte e lo fa attraverso il protocollo di seguito descritto, basato su primitive di crittografia simmetrica. Alice e Bob condividono una master key di lungo periodo K.

A -> B: (A, B) { Alice vuole inviare un file a Bob }
B -> A: K(R) { R = timestamp || nonce }
A -> B: K(R, Ks, N) { Ks è chiave di sessione e N nuovo nonce, entrambi generati da Alice }
B -> A: Ks(N)
A -> B: Ks(<file>)

Si richiede di modificare il protocollo, rispettandone la filosofia, in maniera da garantire anche l'integrità del file inviato. Si assuma che Alice e Bob abbiano concordato l'uso di una certa funzione di hashing H fortemente resistente alle collisioni che trasforma messaggi di m byte in messaggi di k byte, con m e k prefissati e $m \gg k$; si assuma anche $M \gg m$. Discutere la soluzione proposta.

2. Gioco "alto-basso"

a. Alice e Bob decidono di svolgere alcune partite ad "alto-basso", gioco che vede due giocatori scegliere, autonomamente e segretamente, un intero nell'insieme {1, 2, ..., N } e poi, a turno, tentare di indovinare il numero scelto dall'avversario. Durante la partita, quando un giocatore riceve un messaggio che specifica un numero G, questi dovrà rispondere in tempo reale con un messaggio che indichi se G è effettivamente il numero segreto oppure, qualora non lo sia, se G è troppo alto o troppo basso; inoltre, nella stessa risposta, il giocatore potrà a sua volta tentare un numero. Vince chi indovina per primo il numero dell'avversario. E' inoltre stabilito che chi propone la partita definisce l'intervallo {1, 2, ..., N} ma sarà il suo avversario a giocare per primo.
Esempio di protocollo, in cui Alice sfida Bob:

A -> B: (A, B, N) { Alice propone a Bob una partita sull'intervallo 1..N }
B -> A: (B, G) { Bob accetta e "tenta" il numero G }

le possibili risposte di Alice sono nel formato RISPOSTA:

(G, "alto", H) { G è troppo alto; io propongo H }
(G, "basso", H) { G è troppo basso; io propongo H }
(G, "esatto") { G è esatto, ho perso }

A sua volta Bob invierà ad Alice messaggi nel formato RISPOSTA. Al termine della partita il vincitore deve inviare all'avversario un messaggio (<id>, <numero_segreto>), per dimostrare la correttezza delle risposte precedentemente fornite.
Discutere le debolezze del protocollo rispetto a *possibili comportamenti fraudolenti di Alice e/o Bob*.
b. Modificare il protocollo precedente per rimuovere le debolezze riscontrate. Discutere il protocollo risultante.

3. Commercio elettronico

a. Illustrare le caratteristiche generali della specifica SET (Secure Electronic Transaction) descrivendo in dettaglio lo schema della "dual signature" ed evidenziandone l'ambito di uso ed i relativi vantaggi.
b. Descrivere la struttura del messaggio "richiesta di acquisto" ("purchase request") inviata dal cliente al mercante e spiegare perché risulta difficile per il mercante ricavarne il numero della carta di credito del cliente.

4. Firewall

a. Descrivere le caratteristiche degli approcci al firewalling basati su packet filtering, session filtering, circuit-level gateway e application-level gateway, confrontandoli in termini di sicurezza ed efficienza e chiarendo quali siano alcuni possibili requisiti di sicurezza che non possono essere comunque soddisfatti tramite l'uso di firewall.
b. Una rete privata aziendale che deve offrire all'esterno servizi Web e di ricezione email, è organizzata secondo lo schema "screened subnet" ed usa due router capaci di effettuare packet e sesison filtering. Disegnare uno schema della rete e discutere la analogie/differenze nelle impostazioni delle regole di filtraggio dei due router.

5. Domande brevi (al più 8 linee e una figura per risposta)

a. Con riferimento ai problemi di sicurezza a livello di applicazioni Web, discutere brevemente gli elementi rilevanti in merito alla configurazione del Web server.
b. Con riferimento ad IPSec, confrontare i due bundle: *AH (esterno) + ESP (interno) in adiacenza di trasporto* e *AH (interno) in modalità trasporto + ESP (esterno) in modalità tunnel*.