Sicurezza nelle reti e nei sistemi informatici, esame del 20-2-2012. Tempo: 2 ore

1. **Rispondere brevemente alle domande seguenti**
   1.1. La creazione di un canale di comunicazione sicuro fra due parti estranee fra loro su una rete insicura richiede il supporto di terze parti: un KDC (key distribution center) o una CA (certification authority). Quali sono i relativi vantaggi di ciascun approccio? Per quale tipo di reti ciascun approccio è più adatto?
   1.2. Spiegare se un firewall stateless ha la capacità di bloccare richieste di apertura di una connessione TCP da un host esterno verso un host locale, consentendo tuttavia il flusso del traffico verso lo host esterno se la connessione è stata iniziata dallo host locale.
   1.3. In cosa consiste la maggiore robustezza del protocollo EKE in confronto allo schema hash di Lamport?

2. **RSA**
   2.1. La chiave pubblica di Alice è (n, e), dove n = 667 = 23×29 ed e = 3. Assumere l'implementazione "didattica" (da libro di testo) di RSA. Qual è la chiave privata di Alice? Se Bob vuole inviare ad Alice il messaggio 5 cifrato usando la chiave pubblica di Alice, cosa dovrebbe mandare Bob ad Alice?
   2.2. Nella domanda precedente potrebbe insorgere un problema se si utilizza davvero l'implementazione didattica di RSA: spiegare il problema e come questo sia affrontato in PKCS.
   2.3. Quale problema insorgerebbe con l'implementazione didattica di RSA se alcune persone utilizzano per la chiave pubblica lo stesso esponente e=5 e Alice sta inviando lo stesso messaggio (cifrato, per confidenzialità) a tutte loro?

3. **Autenticazione**
   3.1. Descrivere in dettaglio lo hash di Lamport, il suo funzionamento e i suoi punti di forza.
   3.2. Illustrare il meccanismo di autenticazione basato su chiave pubblica e X509, discutendo le principali caratteristiche del protocollo.

4. **SSL e IPSEC**
   4.1. Cos'è una virtual private network (VPN)? Come può IPsec aiutare a creare una VPN?
   4.2. Un'azienda due gateway GW1 e GW2 su due differenti rami della propria rete. Questi consentono agli host dei due rami differenti di comunicare in maniera sicura su Internet attraverso l'implementazione di IPsec solo a livello dei gateway. Quando uno host A della prima rete invia un datagramma a uno host B della seconda rete il gateway GW1 intercetta il datagramma in transito e lo incapsula dentro un pacchetto IPsec. Sull'altro ramo GW2 ricostruisce il datagramma originale e lo invia allo host B instradandolo all'interno della seconda rete.
   Quale dei modi IPsec (tunnel o trasporto) e quale fra i protocolli AH e ESP dovrebbero essere utilizzati se si desidera evitare che un attaccante passivo su Internet conosca le identità degli host A e B?
   4.3. L'attacco *rogue packet* contro SSL è il seguente. L'attaccante sniffa il traffico fra le due parti e crea un segmento TCP valido per la connessione (numero di sequenza e checksum entrambi corretti).
   Descrivere le possibili conseguenze dell'attacco (suggerimento: SSL si appoggia direttamente su TCP).

5. **Sicurezza del browser**
   5.1. Illustrare il meccanismo dei cookie, le varie tipologie di cookie e i più frequenti problemi legati al loro uso.
   5.2. Spiegare come i cookie possano essere sfruttati lato server per tracciare la navigazione di un utente attraverso più siti. Come si può contrastare il tracciamento?