

# Esercizi

Quando si inviano pacchetti da firewall a firewall si introduce un nuovo IP header. E' necessario?

- si: perche' ogni Security association definisce le proprie chiavi; se A manda a B un messaggio e la rete di A ha un firewall F e la rete locale di B ha due firewall F1,F2(piu' di un accesso a internet) allora il messaggio codificato con la chiave condivisa da F e F1 potrebbe giungere a F2 (e viceversa).
- e' anche opportuno perche' in questo modo si nasconde il traffico fra gli effettivi utenti

A manda pacchetti a B con IPSEC. ACK mandato da TCP di B e' perso, quindi A invia di nuovo il pacchetto. Chi si accorge del duplicato?

- IPSEC non si accorge del duplicato che viene riconosciuto da TCP di B

In alcuni sistemi si usano diversi tipi di chiavi: chiavi segrete condivise, chiavi pubbliche di firma, chiavi pubbl. di codifica.

### Vantaggi e svantaggi

- chiavi segrete predeterminate
- chiavi di firma
- chiavi di codifica

In alcuni sistemi si usano diversi tipi di chiavi: chiavi segrete condivise, chiavi pubbliche di firma, chiavi pubbl. di codifica.

### Vantaggi e svantaggi

- chiavi segrete predeterminate: veloci nel calcolo, veloci da immettere (se utente umano), Piu' complesso da configurare (si richiede una chiave per ogni coppia di utenti)
- chiavi di firma: difficili da falsificare, piu' lente; non ci sono problemi di esportazione
- chiavi di codifica: difficili da falsificare, problemi di esportazione; un vantaggio rispetto a chiavi di firma è che in questo modo si nasconde l'identità degli utenti

## Confronta i seguenti metodi per ottenere una chiave pubblica in termini di efficienza, sicurezza, ecc

- accesso a nodo con dato IP che conosce con certezza la chiave
- accesso ad un direttorio senza accesso autenticato
- accesso ad un direttorio con accesso autenticato
- ognuno memorizza il suo certificato con tutte la gerarchia

## Confronta i seguenti metodi per ottenere una chiave pubblica in termini di efficienza, sicurezza, ecc

- accesso a nodo con dato IP che conosce con certezza la chiave: poco sicuro, veloce (sicurezza su indirizzo IP)
- accesso ad un direttorio senza autenticazione: attaccante si sostituisce, veloce
- accesso ad un direttorio con accesso autenticato: più lento, sicuro (problema: direttorio deve essere sicuro)
- ognuno memorizza il suo certificato con tutte la gerarchia: molto lento (certificati forniti da B prima di iniziare qualunque cosa)

Si consideri il seguente protocollo per autentica e per stabilire una chiave segreta comune. Si utilizza chiave pubblica

- A a B :  $\text{Sig}_A(\text{KPB}(K), T)$  ( $\text{Sig}_A$ : firma di A, K chiave proposta, T timestamp, KPB chiave pubb. B)
- B a A :  $K(T)$

Sicuro? chiave K è comune o e' nota ad altri?

SI: B riconosce A in base alla firma del timestamp

A riconosce B perché mostra di conoscere T, e quindi la sua chiave segreta; K è noto solo a chi conosce la chiave segreta di B

# Progetta un protocollo di Diffie-Hellman in cui A ha chiave di firma e B ha chiave pubblica di codifica

Suggerimento: uso di funzioni hash

- A a B: Alice,  $KPB(g^a \text{ mod } p)$ ,  $Sig\_A(KPB(g^a \text{ mod } p))$   
(solo B puo' leggere; la firma di A garantisce  $g^a$ )
- B a A:  $g^b \text{ mod } p$ ,  $hash(g^{ab} \text{ mod } p)$   
(A calcola  $g^{ab}$  e verifica conoscenza di B)
- A a B:  $hash'(g^{ab} \text{ mod } p)$   
(B verifica che A conosce la chiave)

## Regole di buon senso

- cambiare le chiavi frequentemente (se non possibile uso di chiavi di sessione temporanee)
- usa chiavi differenti nelle due direzioni (rende piu' difficili attacchi basati sul rispedito messaggi vecchi)
- uso di chiavi diverse per codifica e per integrita'
- in generale usa chiavi diverse per ogni scopo specifico: questo provoca problemi nel senso che non sempre le applicazioni usano la chiave giusta. soluz. padding specifici per applicazione

## Regole di buon senso -2

- in comunicazione fra due utenti ognuno determina la chiave: non solo per fiducia, ma anche per evitare che se un attaccante si sostituisce non sia poi in grado di fornire la chiave di sessione da solo (se la chiave di sessione è il contributo di ciascuno, che viene mandato crittato)
- uso di generatori di numeri casuali a partire da un seme iniziale;
- diffidare di soluzioni hardware per la generazione di numeri casuali