Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova scritta

Mauro Brunato

Lunedì 24 luglio 2017

Esercizio 1

1.1) Descrivere il protocollo Diffie-Hellman per la generazione di una chiave condivisa.

1.2) Come mai, pur potendo intercettare tutti i messaggi in chiaro, una terza parte non è in grado di ricostruire la chiave?

1.3) Descrivere una possibile tecnica di attacco al protocollo.

Esercizio 2

Per autenticare i messaggi che spedisce a Bob, Alice utilizza un sistema di firma digitale basato su una funzione hash $H(\cdot)$ e la funzione RSA di cifratura a chiave pubblica $\mathrm{RSA}_K(\cdot)$, dove K può essere una chiave pubblica o privata.

2.1) Supponendo che Alice non sia interessata alla confidenzialità, come sarà composta la firma s che Alice concatenerà al messaggio m per certificarne l'autenticità? Si assuma che Bob conosca già la chiave pubblica di Alice.

2.2) Supponiamo ora che sia la funzione hash, sia le chiavi di Alice, siano a 32 bit, quindi molto brevi. Se Charlie desidera inviare un messaggio specifico m' a Bob, come può procedere per forza bruta?

2.3) Sappiamo che RSA è un algoritmo abbastanza lento; supponendo che il computer di Charlie possa calcolare 10^3 funzioni RSA al secondo e 10^9 funzioni hash al secondo, quanto tempo impiegherà mediamente a forgiare una firma di Alice con l'attacco a forza bruta descritto al punto precedente?

Suggerimento — *Come al solito, è lecito utilizzare l'approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Una piccola rete locale è costituita da un'intranet a indirizzi privati e da un router in grado di eseguire NAT e port forwarding. Il router possiede un'interfaccia WAN `s0` e un'interfaccia Ethernet `e0`. Una delle macchine dell'intranet, che chiameremo P, ha in esecuzione un proxy applicativo in grado di supportare comunicazioni HTTP. Questa macchina è l'unica autorizzata a comunicare con l'esterno. Tutte le altre macchine dell'intranet possono comunicare con l'esterno solo tramite P.
L'interfaccia `s0` del router ha ricevuto l'indirizzo `35.143.22.228/29` e deve utilizzare come default gateway l'indirizzo più alto assegnabile a un host nella stessa sottorete.

3.1) Disegnare uno schema di massima della rete; illustrare la configurazione di una macchina generica dell'intranet e del proxy P.

3.2) Illustrare la configurazione del router: interfacce di rete, tabella di instradamento, NAT, eventuali ACL.

3.3) Descrivere per sommi capi come avviene una richiesta HTTP da parte di un host dell'intranet (diverso da P) verso un server remoto.