Sicurezza nelle Reti

Appello del 3 Novembre 2006

Nome e Cognome_____**Matricola** _____

QUESITO 1 — PUNTI: 12 (6, 3, 3)

Con proprietà di linguaggio e precisione matematica, si risponda alle seguenti domande.

1. Si definisca la funzione hash con chiave (Message Authentication Code, MAC).
2. Si consideri una funzione hash con chiave h caratterizzata come segue: 1) la chiave è su t bit; 2) l'output è su n bit; 3) l'output della funzione hash può essere considerato una variabile aleatoria uniformemente distribuita.
   i. Un avversario ha a disposizione una coppia $(x, h_k(x))$ e tenta un attacco esaustivo allo spazio candidato. Si chiama *falso positivo*, una chiave z, diversa da k, tale che $h_z(x) = h_k(x)$. Qual è il numero medio di falsi positivi che ci si aspetta da un attacco esaustivo allo spazio delle chiavi? (si assuma che $2^t \gg 1$ e $2^n \gg 1$).
   ii. Quante coppie $(x_i, h_k(x_i))$ sono necessarie per eliminare il problema dei falsi positivi ovvero di ridurre il loro numero aspettato ad un valore minore di uno?

SOLUZIONE

Quesito 1. Vedere appunti.

Quesito 2. Con chiavi a t bit si possono fare 2^t tentativi: 1) calcolare $h_i(x)$ e 2) verificare se il valore ottenuto è uguale a $h_k(x)$ per ogni valore di i, $0 \le i < 2^t$. Uno di questi tentativi produrrà alla chiave cercata. Gli altri 2^t-1 tentativi possono produrre un falso positivo. Siccome la funzione hash produce un output perfettamente random per ipotesi, allora per ogni tentativo si ha una probabilità pari a 2^{-n} di produrre un falso positivo. Per cui mediamente ci si aspettano $(2^t-1)/2^n$ falsi positivi.

Quesito 3. Supponiamo adesso di avere r coppie $\left(x_i, h_k\left(x_i\right)\right), 1 \le i \le r$. Nei 2^t tentativi, ce ne sarà uno, quello relativo alla chiave k. Per avere un falso positivo z bisogna che $h_z\left(x_i\right) = h_k\left(x_i\right), \forall i \in \left[1, r\right]$. Data una chiave z, la probabilità che questo accada è data dalla probabilità composta ed è perciò pari a $\prod_{i=1}^{r} \mathcal{P}\left(h_z\left(x_i\right) = h_k\left(x_i\right)\right) = 2^{-rn}$. Ne segue che il numero medio di falsi positivi è $\left(2^t - 1\right) \times 2^{-rn} \approx 2^{t-rn}$. Per escludere la possibilità di falsi positivi basta imporre $2^{t-rn} < 1$ che è verificata per $r > t / n$.

QUESITO 2 — PUNTI: 12 (3, (3, 3), 3)

Si consideri il seguente protocollo di distribuzione delle chiavi.

M1 $A \rightarrow B$: $E_e\left(k\right)$

M2 $B \rightarrow A$ $S_B\left(E_e\left(k\right)\right)$

dove k è una chiave di sessione, e è una chiave per comunicare in maniera confidenziale con B ed S è una firma digitale. Oltre a distribuire una chiave di sessione, il protocollo ha l'obiettivo di identificare B rispetto ad A (ma non viceversa). Il candidato risponda alle seguenti domande con precisione e proprietà di linguaggio.

1. Sotto quali ipotesi il protocollo garantisce l'identificazione di *B* rispetto ad *A*?
2. Si assuma che *E* ed *S* siano realizzati per mezzo dell'algoritmo RSA.
    a. È possibile utilizzare la stessa coppia di chiavi pubblica (e_B, n_B) e privata (d_B, n_B) sia per *E* sia per *S*?
    b. Nel caso si utilizzino due coppie di chiavi diverse quale relazione deve sussistere tra i moduli? Si indichi con n_e e con n_s i moduli per il cifrario e per la firma digitale rispettivamente.
3. Si modifichi il protocollo in modo da utilizzare, come crittografia asimmetrica, solo il cifrario *E*.

QUESITO 3 — PUNTI: 6

Si descriva il processo di generazione dell'intestazione ESP.