# Esame di Reti di Calcolatori e Sicurezza

Soluzione

18 settembre 2006

1. L'accesso al canale di una certa LAN avviene con ALOHA slotted. Tutti i frame hanno durata di 1 ms, pari al tempo di slot e sulla rete si trovano 20 stazioni, e sul canale si osserva un tasso di 2 trasmissioni tentate per ogni slot.

   (a) Quanti frame al secondo riesce a trasmettere con successo ogni stazione?

   (b) Qual è il tempo medio di servizio per ogni pacchetto generato da una stazione?

   (c) Cosa bisognerebbe fare per migliorare le prestazioni (aumentare la capacità di trasporto e diminuire il tempo di servizio)?

   **Risposta:**

   (a) (2pt) $G = 2$, quindi $S = Ge^{-G} = 2e^{-2} = 0,2707$. Dato che ci sono 1000 slot in un secondo, ogni secondo hanno successo circa 270,7 trasmissioni fra tutte le stazioni; quindi ogni stazione riesce a trasmettere 13,53 frame al secondo (comprese le ritrasmissioni).

   (b) (2pt) In media, il numero di tentativi necessari per spedire un pacchetto è $E = e^G = 7,39$. Ogni tentativo impiega 1 ms, quindi il tempo di servizio medio è 7,39 ms.

   (c) (2pt) In generale, affinché il canale non sia sovraccarico ci deve essere meno di 1 tentativo per slot ($G \leq 1$), quindi bisogna diminuire il numero di richieste per slot. Per esempio, diminuendo le stazioni o aumentando il numero di slot (diminuendo il tempo di frame).

2. Nelle reti Bluetooth:

   (a) Quale tecnica di trasmissione viene utilizzata, e perché?

   (b) Si ricordi che i circuiti radio impiegano circa 250 $\mu$s per assestarsi su una frequenza; ogni frame ha una intestazione di 126 bit.

   Quale è il transfer rate massimo da un nodo slave verso il master (o viceversa)?

   (c) E da uno slave all'altro?

   **Risposta:**

   (a) (2pt) Utilizza la FHSS (Frequency Hopping Spread Spectrum) su 79 canali nella banda ISM dei 2.4 GHz, con hop time di 625 $\mu$s (1600 hop/s). Uno slot occupa un canale per il tempo di un hop. La codifica è FSK, ad 1 bit/Hz. Si usa questa tecnica per aumentare la resistenza ai disturbi e alle interferenze.

   (b) (3pt) Un frame può occupare 1, 3 o 5 slot consecutivi. Il caso ottimo è quando lo slave usa 5 slot consecutivi, e poi il master occupa solo 1 slot. Complessivamente questo ciclo occupa $6 \times 625 = 3750\mu$s. Nei 5 slot, lo slave trasmette al massimo 2744 bit (v. fig. 4.38 sul Tanenbaum). (Se uno non si ricorda questo valore, lo si ricava considerando che bisogna togliere 250 $\mu$s per l'assestamento e 126 per l'intestazione; rimangono $5 \times 625 - (250 + 126) = 2749\mu$s, da cui si tolgono 5 $\mu$s per sicurezza.) Quindi il datarate è $2744/3750 \cdot 10^{-6} = 731733$ bps = 714 kbps = 89,3 kB/s.

   (c) (2pt) Nel Bluetooth non c'è comunicazione diretta tra slave; tutto deve passare per il master. Il caso migliore è quando lo slave mittente spedisce al master un frame da 2744 bit (che occupa 5 slot), e subito dopo il master lo inoltra allo slave destinatario (occupando altri 5 slot). In totale questo ciclo prende 10 slot = 6250 $\mu$s, per trasmettere 2744 bit. Il datarate è quindi $2744/6250 \cdot 10^{-6} = 439040$ bps = 428,75 kbps = 53,6 kB/s.

3. (a) Si descriva la creazione delle chiavi nel cifrario RSA.

   (b) Quali sono i vantaggi rispetto agli schemi di cifratura simmetrica (o a chiave privata)?

   (c) Perché gli schemi di cifratura simmetrica sono ancora molto usati?

   **Risposta:**

   (a) (3pt) RSA è un cifrario a chiave pubblica basato sulla teoria dei numeri primi. Per

generare una coppia di chiavi, si scelgono due numeri primi $p, q$, si calcola il loro prodotto $n = pq$ e si scelgono due numeri $e, d$ tale che $1 < e < \phi(n)$, $e$ è primo rispetto a $\phi(n)$ e $ed = 1 \bmod \phi(n)$ (dove $\phi(n) = (p-1)(q-1)$). La chiave pubblica è $(e, n)$, la chiave privata è $(d, n)$. Dato un messaggio in chiaro $M$, $0 \leq M < n$, il corrispondente messaggio cifrato è $C = M^e \bmod n$; dato un messaggio $C$ cifrato con $(e, n)$, il corrispondente messaggio in chiaro è $M = C^d \bmod n$.

(b) (2pt) Come ogni schema asimmetrico, permette lo scambio di informazioni cifrate tra due parti (in una direzione) senza che questi si siano scambiati preventivamente una chiave segreta. Lo scambio è monodirezionale perché la chiave pubblica di $A$ può essere usata da $B$ per spedire un messaggio ad $A$, ma non viceversa.

(c) (2pt) Per motivi di efficienza. Gli algoritmi di cifratura asimmetrica noti sono molto pesanti, e richiedono chiavi molto lunghe (migliaia di bit); per contro, gli algoritmi di cifratura simmetrica sono molto efficienti e offrono ottima robustezza già con 128 bit. Per cui, la maggior parte delle volte la cifratura simmetrica viene usata solamente per stabilire una chiave di sessione per un cifrario simmetrico (p.e., DES o AES).

4. Si discuta se e come i seguenti attacchi vengono sventate dall'uso di SSL:

   (a) Attacco a dizionario con testo in chiaro noto (p.e., l'intestazione del protocollo HTTP).

   (b) Attacco a ripetizione della fase di handshake

   (c) Sniffing delle password a livello utente (p.e., quelle usate nell'autenticazione HTTP o SMTP)

   (d) Attacco Denial of Service di tipo "SYN flooding"

   **Risposta:**

   (a) (2pt) Le chiavi di sessione sono sufficientemente lunghe da rendere questo attacco non praticabile. Per esempio, con chiavi di 128 bit bisogna avere $2^{128}$ entry.

   (b) (2pt) Sia il client, sia il server generano due nonces univoche (che contengono anche il timestamp); tali nonces vengono usate per generare, assieme alla secret master key, le chiavi di sessione. Se un intruder prova a ripetere un handshake usando la stessa nonce (del client), la controparte genera una nonce diversa dalla precedente e quindi la master key e tutte le chiavi di sessione cambiano.

   (c) (1pt) I dati trasportati sono cifrati.

   (d) (2pt) SSL non offre protezione da questo attacco.

5. [Da sviluppare su un foglio a parte]

   Si descriva dettagliatamente l'attacco "ARP poisoning", disegnando anche un apposito schema di rete rappresentativo. In particolare, si spieghi qual è lo scopo dell'attacco, quali vulnerabilità sfrutta, come ("step-by-step") viene effettuato, quali sono gli impatti e i possibili rimedi.