TELEMATICA
PROVA SCRITTA

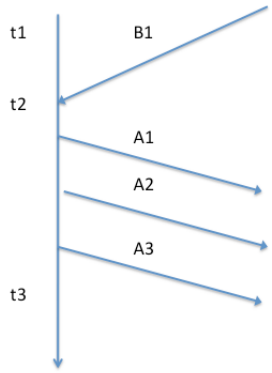
14 Gennaio 2013
Tempo a disposizione 120 Minuti

Es 1 (8 pt) Consideriamo un messaggio di posta elettronica con mittente alice@unipi.it, destinatario bob@cs.mit.edu e testo del messaggio "Cervello in fuga!!" Indicare il contenuto dei primi tre segmenti TCP inviati dal mailserver smtp.cs.mit.edu per ricevere tale messaggio, specificando di tutti i segmenti sia il contenuto della parte dati che i valori dei campi numero di porta origine, numero di porta destinazione, numero di sequenza, numero di riscontro ed eventuali bit di tipo flag a 1.

Es 2 (12 pt)
Supponiamo che al tempo t1 il TCP di un processo applicativo A abbia 3 MSS di dati in volo, che il valore di sendBase sia X, che la dimensione della sua finestra di congestione sia 3MSS e che abbia altri 3 MSS di nuovi dati da spedire.
Supponiamo inoltre che, quando riceve il segmento B1 che è un riscontro che non contiene dati, il TCP di A invii tre segmenti (A1, A2 e A3) contenenti rispettivamente 1MSS, 1MSS e 1/3MSS di nuovi dati. Supponendo che nell'intervallo [t1,t3] il TCP di A riceva e invii solo i segmenti indicati nella figura a lato e che in tale intervallo non scada nessun timeout.
Indicare, giustificando la risposta:

- i possibili valori di AckNum e di RcvWin contenuti in B1,
- i possibili valori di SeqNum in A1, A2 e A3
- i possibili valori di CongWin, SendBase e NextSeqNum in t3.

Si consideri sia nel caso in cui A si trovi nello stato di slow start che nello stato di congestion avoidance.
Per semplicità supponiamo che tutti i segmenti contenenti dati scambiati da A e B (ad eccezione di A3) contengano 1 MSS di dati.



Es 3 (6 pt) Supponiamo che Bob e Alice abbiamo la possibilita' di utilizzare un sistema crittografico che mette a disposizione le loro chiavi pubbliche. Supponiamo inoltre che Bob voglia firmare digitalmente un documento D.

a) Quali sono le operazioni che Bob deve compiere per firmare il documento D?
b) Bob invia il documento firmato digitalmente a Alice. Quali sono le operazioni che deve compiere Alice per autenticare Bob come firmatario del documento?

Es 4 (6 pt) Consideriamo una rete locale con un unico router gateway di interfaccia. Sotto quale ipotesi e' possibile determinare tutte le connessioni che lo attraversano? Si motivi la risposta.

TRACCIA SOLUZIONE.

Es1. Il primo segmento inviato dal mailserver sara' un segmento di tipo "SYNACK" contenente:

portaOrigine = 25
portaDestinazione = P
SEQ = Y
ACK= X+1
bit SYN e ACK a 1
DATI: nessun dato spedito

dove P e' il numero di porta del cliente e Y e X sono i numeri di sequenza inziali scelti dal server smtp.unipi.it e dal client, rispettivamente.

Secondo Segmento

portaOrigine = 25
portaDestinazione = P
SEQ = Y+1
ACK= X+1
DATI: 220 smtp.cs.mit.edu

Terzo segmento

portaOrigine = 25
portaDestinazione = P
SEQ Y+ 1 + k dove k = length(Header SMTP +220 smtp.cs.mit.edu)
ACK = X+1 + k' dove k' = length(Header SMTP + HELO smtp.cs.mit.edu**)**
Dati: 250 Hello smtp.unipi.it pleased to meet you

Es2. Dato che al tempo t2 il TCP di A spedisce dei nuovi messaggi, il riscontro B1 deve essere necessariamente un riscontro positivo. Abbiamo due casi

- TCP di A si trova nello stato di slow start. Al momento della ricezione di B1 il valore di CongWin diventa 4 MSS. Abbbiamo diversi casi. Prima di tutto si deve notare che il valore di B1.ACK deve essere necessariamente maggiore o uguale a X+2MSS perche' altrimenti il TCP di A non potrebbe mandare 2MMS + 1/3MSS di nuovi dati (se B1/ACK fosse uguale a X+1 MSS allora A avrebbe ancora due MSS in volo e quindi non potrebbe inviare i nuovi dati). Quindi i casi da considerare sono:
    - B1.ACK = X+2MSS allora A ha ancora un MSS di dati in volo, pertanto 1MSS + 2 MSS + 1/3 MSS <= min(CongWin, B1.RCW) questo implica che 3MSS+ 1/3 MSS <= min(4MSS, B1.RCW). Da cui si deriva che B1.RCW = 3MSS + 1/3 MSS
    - B1.ACK = X+3MSS allora A non ha alcun dato in volo, pertanto 2 MSS + 1/3 MSS <= min(CongWin, B1.RCW) questo implica che 2MSS+ 1/3 MSS <= min(4MSS, B1.RCW). Da cui si deriva che B1.RCW = 2MSS +1/3 MSS

    - TCP si trova nello stato di congestion avoidance. Al momento della ricezione di B1 il valore di CongWin diventa 3 MSS + 1/3MSS.
        - B1.ACK = X+2MSS allora A ha ancora un MSS di dati in volo, pertanto 1MSS + 2 MSS + 1/3 MSS <= min(CongWin, B1.RCW)

questo implica che 3MSS+ 1/3 MSS <= min(3MSS+ 1/3 MSS, B1.RCW). Da cui si deriva che B1.RCW >= 3MSS + 1/3 MSS

- B1.ACK = X+3MSS allora A non ha alcun dato in volo, pertanto 2 MSS + 1/3 MSS <= min(CongWin, B1.RCW) questo implica che 2MSS+ 1/3 MSS <= min(3MSS+ 1/3 MSS, B1.RCW). Da cui si deriva che B1.RCW = 2MSS +1/3 MSS

Es3. Bob deve codificare il documento D (o per meglio dire un hash di D) con la sua chiave privata (KBob-). Bob invia a Alice la coppia (D, KBob-(D))
Alice riceve la coppia (D, C). Decodifica C con la chiave pubblica di Bob KBob+(C) ottenendo D'. Se D' = D allora Alice autentica Bob come firmatario del documento
Es4. In generale i router sono staless contengono solamente la tabella di inoltro. Nel caso in cui il router operi come NAT, allora la NAT table contiene tutte le informazioni per determinare quali e quante sono le connessioni che attraversano il router.