15-441 Computer Networks
Homework #4
Out: 04/12/05 Due: 1:30 PM 04/26/05
Lead TA: Debabrata Dash (ddash+@cs.cmu.edu)

1 TCP

1. In the class we saw the relationship between bandwidth achieved by TCP and the loss rate. Suppose in the congestion avoidance state TCP increases the window by 2 MSS instead of 1 and on congestion loss it multiplies the window size by 0.75 instead of 0.5. What would be the new relationship between bandwidth and loss rate?

2. [Peterson & Davie 5.39] When TCP sends a (SYN,SequenceNum = x) or (FIN, SequenceNum = x), the consequent ACK has Acknowledgement = x + 1; that is, SYNs and FINs each take up one unit in sequence number space. Is this necessary? If so, give an example of an ambiguity that would arise if the corresponding Acknowledgement were x instead of x + 1; if not, explain why?

2 QoS

1. Consider 10 flows with arrival rates of 1, 2, ..., 10 Mbps that traverse a link of 50Mbps. Compute the max-min fair share on this link. What is the fair share if the link capacity is 60 Mbps?

2. Suppose a router has accepted flows with the token bucket parameters shown in Table 1. All flows are in the same direction, and the router can forward one packet every 0.1 seconds.

   (a) What is the maximum delay a packet might face?

   (b) What is the minimum number of packets from the third flow that the router would send over 2.0 seconds, assuming that the flow sent packets at its maximum rate (4 Packets/sec) uniformly?

Token Rate	Bucket Size
1	10
2	4
4	1

Table 1: Token Bucket Parameters

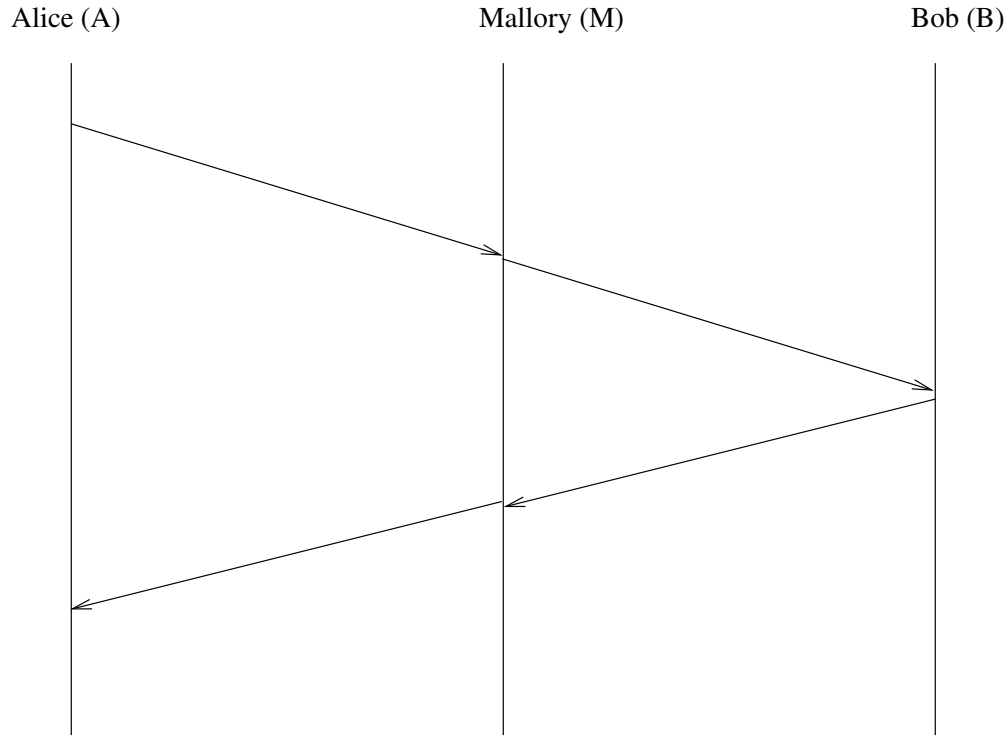

Figure 1: Figure for Question 3-1

3 Security

1. For over ten years, the following protocol was thought to be secure. It is a protocol that allows two people, X and Y, to authenticate themselves to each other. Let K_X, K_X^{-1} and K_Y, K_Y^{-1} be the public and private keys of X and Y, respectively. Let N_* be a nonce (i.e. a random number) generated by node $*$. Let the notation $[M]_{K_X}$ mean that the message M is encrypted using key K_X. The protocol is then:

$$X \to Y : [N_X, X]_{K_Y}$$
$$Y \to X : [N_X, N_Y]_{K_X}$$
$$X \to Y : [N_Y]_{K_Y}$$

Alice wants to authenticate herself to Mallory using the above protocol in order to send Mallory a postcard. Mallory, however, being the unscrupulous person she is, can use Alice s gesture of friendship to turn around and impersonate Alice to Bob-the-banker! Once Mallory has authenticated herself to Bob as Alice, she can then transfer money from Alice s account to her own, or do other nefarious deeds.

(a) Show how Mallory is able to impersonate Alice by writing each line in the packet

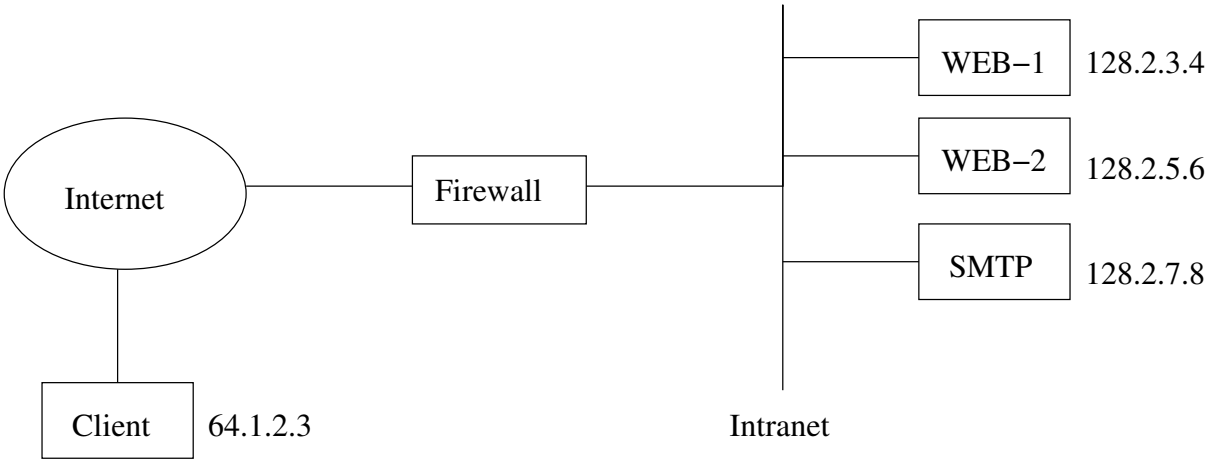

Figure 2: Network topology for Question 3-2

exchange diagram (Figure 1) the message that would be sent.

(b) Explain how the protocol can be made secure against this attack, and show a packet exchange diagram for your modified protocol.

(c) If Alice, Mallory and Bob are all computers on an Internet, explain where Mallory must be located with respect to Alice and Bob to carry out her attack, and how she might be able to accomplish it.

2. Consider the firewall scenario depicted in Figure 2. In Table 2, fill the values that achieve the following policy. Assume that policy items not mentioned below are disallowed and the firewall is a stateless packet filter. Note that you may need less number of rows than what is provided in Table 2.

   - Any external host can access HTTP Server WEB-1.
   - Any external host can access the SMTP server.
   - Only the HTTP client shown can access HTTP Server WEB-2.
   - Kazaa is allowed between any internal and external peers, in either direction, except for the SMTP server.
   - HTTP is allowed from any internal host to any external host.
   - Outgoing SMTP is allowed only from the SMTP Server.

4 Wireless

1. Lets say we are running TCP over a wireless link. We learned in the class that the link layer can retransmit locally to enable better TCP performance. Suppose the link layer transmits 5 times before reporting a loss to upper layer and does exponential back-off after each loss (starting at 2ms and doubling each time). The wireless link has a 10% loss rate, and the delay between the end points is 2ms.

Rule	Dir	Src IP	Src Port	Dst IP	Dst Port	Protocol	Ack Set?	Action

Table 2: Table for Question 3-2

(a) What would be the expected delay seen by the upper layers?

(b) What would be the expected mean RTT deviation seen by the end hosts?

(c) What would be the expected RTO seen by the end hosts on a TCP connection over this wireless network? Assume that in the steady state the delay seen by the end hosts is the expected delay seen in (a).

2. We learned about hidden terminal and exposed terminal problems and fixing them by using RTS/CTS control messages.

(a) Suppose a node wants to transmit, explain if it should transmit or hold if it receives *(i)* just an RTS (no corresponding CTS) *(ii)* just a CTS (no corresponding RTS) *(iii)* Both RTS and the corresponding CTS.

(b) Your friend claims that RTS/CTS control messages are not needed in his network as the DATA and ACK packet sizes are small (almost the same size as RTS/CTS packets). Why is he right?

(c) You also discovered that, the CMU administrators have turned off the RTS/CTS mechanism in all wireless cards (even though the DATA packets are not that small). Why is that ok?

5 CDN

1. A browser on system A accesses `index.html` at `www.cnn.com`. Suppose CNN use Akamai to distribute its images and there are two images in the `index.html` named `A.gif` and `B.gif`. Akamai uses TTLs of 1 day, 30 minutes and 20 seconds for high-level DNS server NS records, low-level DNS server NS records and host address records, respectively. The local DNS server for the system is called D. Assuming that the browser's cache and DNS cache on D are empty. List the sequence of HTTP and DNS requests issued by A and D.