CSE331: Introduction to Networks and Security **Midterm**
Fall 2004 **Oct. 11, 2004**

1	/10
2	/30
3	/28
4	/18
5	/9
6	/5
Total	/100

- Do not begin the exam until you are told to do so.
- You have 50 minutes to complete the exam.
- There are 7 single-sided pages; please sign your name on *all* of them.

1. (10 points) True or False?

Circle the appropriate answer.

a. T F Denial of service attacks against a web server can be prevented by having the web server handle only a fixed number of requests at any given time.

b. T F One second is enough time for approximately 10 round trips from the east coast to the west coast of the United States on the Internet.

c. T F The trusted computing base is made up of those components that have been certified not to fail.

d. T F If host A's IP address is 158.63.16.60 and Host B's IP address is 158.63.16.128, and both hosts are configured with the subnet mask 255.255.255.192, then they are on the same subnet.

e. T F The principle of complete mediation suggests that a web server should be configured so that its SMTP port (port 25) is turned off.

f. T F One advantage of virtual circuit routing over the datagram model is that it provides better guarantees about the quality of network service.

g. T F IPv4 provides congestion control mechanisms such as additive increase/exponential decrease to improve the overall performance of the Internet.

h. T F Both subnetting and network address translation can help with the problem of network scalability.

i. T F Buffer overflows and similar software errors are the most frequently exploited vulnerabilities on the Internet.

j. T F The domain name system maps host addresses from the network layer of the protocol stack to host addresses at the data link layer.

2. (30 points total) Short answer

Answer each of the following questions using at most a few sentences.

a. (8 points) Give two reasons, other than buffer-overflow attacks, why a network with both a firewall and virus-detection software may still be vulnerable. Assume that both the firewall and the virus scanner are configured correctly with up-to-date information and that all network connections go through the firewall.

i. vulnerability 1:

ii. vulnerability 2:

b. (10 points) The first version of HTTP (1.0) established a separate TCP connection for each data item (i.e. embedded image) retrieved from the server. Most HTTP data items are small—less than one or two KB. Newer versions of HTTP create a persistent TCP connection over which the client and server can exchange multiple request/response messages.

i. Describe two features of the TCP protocol that motivate the change to persistent connections. Justify your answers.

ii. Describe a drawback of the persistent connection approach.

c. (12 points) Consider the operation of a typical e-mail system. Recall that there are three primary qualities (or properties) of data in such a system that security mechanisms are designed to protect. Name each of the qualities, and, for each, give a *one-sentence* example of an attack that violates it.

i. Quality 1:

ii. Quality 2:

iii. Quality 3:

3. (28 points total) Network performance calculations

Show all of your work for full credit.

a. (7 points) Assuming that the send window size (SWS) parameter of the sliding-window algorithm has been optimized for a particular local area network that has a RTT of 10ms and bandwidth of 10Mbps. If SWS is 125, what is the framesize for the network in bytes?

b. Suppose that you want to control one of the Mars rover scientific robots using a direct radio link. Assume that Mars is 210×10^6 kilometers from Earth (Mars' actual orbit means that its distance from Earth varies between about 55×10^6 and 400×10^6 kilometers.) and that the speed-of-light in a vacuum is $3 \times 10^8 m/sec$. The communication channel has a bandwidth of 10Mbps.

i. (7 points) Calculate the minimum RTT for the link in seconds.

ii. (7 points) Using the RTT as the delay, calculate the delay $\times$ bandwidth product for the link in MB.

iii. (7 points) A camera on the rover takes pictures of the Martian landscape and saves them in digital format to disk. Suppose Mission Control on Earth wishes to download the most current image, which is 25MB. What is the minimum amount of time (in seconds) that can elapse between the time that the request for the data goes out from Earth and the transfer is finished? (Assume that the processing time on the rover is negligible.)

4. (18 Points) Firewall Security

Suppose we place a filtering firewall between a LAN and the Internet as shown in the figure below, where the labels on the arrows indicate the physical ports on the firewall router. The LAN hosts inside the firewall have IP addresses described by the regular expression 240.155.16.*.

$$LAN \underset{o_2}{\overset{i_1}{\rightleftarrows}} \boxed{\text{Firewall}} \underset{i_2}{\overset{o_1}{\rightleftarrows}} INTERNET$$

The filter table for port i_2 is:

Line	Action	Source	Port	Dest.	Port
1.	Block	158.214.5.*	80	240.155.16.*	*
2.	Allow	*	80	240.155.16.*	*
3.	Allow	*	*	240.144.16.3	25
4.	Block	*	*	*	*

The filter tables for ports o_1 and o_2 permit *all* traffic.

a. (8 points) For each of the following packet descriptions arriving at port i_2 of the firewall, fill in which line of i_2's filter table will be used to determine whether the packet is Blocked or Allowed. Each answer should be a single number 1, 2, 3, or 4.

Source	Port	Dest.	Port	ANSWER
158.214.5.12	2400	240.155.16.3	23	
128.7.244.129	80	240.155.16.3	6002	
158.214.5.12	25	240.155.16.3	25	
158.214.5.12	80	240.155.16.3	25	

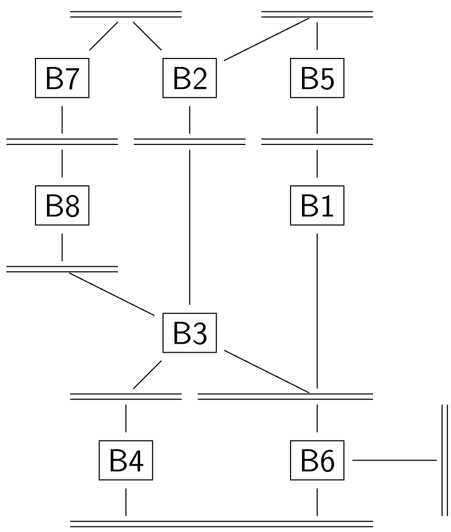
b. (5 points) Suppose that you want the policy on out-bound connections from the LAN to be as liberal as possible while still preventing IP spoofing from with the LAN. Complete the filter table for port i_1 :

Line	Action	Source	Port	Dest.	Port
1.					
2.	Block	*	*	*	*

c. (5 points) Recall that HTTP servers run at port 80. Does the firewall permit a LAN host to establish an HTTP connection with a web server with IP address 158.214.5.12? Explain your answer in one sentence.

5. (9 points) Routing

In the diagram below, there are 7 bridges with identifiers B1–B7 connecting 10 Ethernet links (indicated by the double lines). Ports connecting bridges to Ethernet links are shown by solid lines. Recall that the distributed minimum spanning tree algorithm prefers bridges with smaller identifiers and that the bridge with the smallest identifier is elected as “root”. Assuming that there are no failures in the network and that each hop has the same cost, indicate which ports *do not* participate in the final spanning tree of this network.



6. (5 points) CRC

Consider the CRC error detection scheme with degree 3 divisor polynomial $z^3 + 1$. The sequence of bits transmitted when the original message consists of the sequence 10101010 is (choose one):

1. 10101010000
2. 10101010001
3. 10101010100
4. 10101010111