Name ________________________
Student Number________________________

Software Engineering 4C03

DAY CLASS — Dr. William M. Farmer
DURATION OF EXAMINATION: 2 Hours
MCMASTER UNIVERSITY FINAL EXAMINATION — April 2001

THIS EXAMINATION PAPER INCLUDES 10 PAGES AND 51 QUESTIONS. YOU ARE RESPONSIBLE FOR ENSURING THAT YOUR COPY OF THE PAPER IS COMPLETE. BRING ANY DISCREPANCY TO THE ATTENTION OF YOUR INVIGILATOR.

Special Instructions

The use of any notes and books is permitted during this exam. Answers to the first forty-two questions (1–42) are to be marked on the exam itself as well as on the OMR scan sheet. In case of discrepancies, the scan sheet is considered to be your answer. Answer the last nine questions (42–51) in the space provided on the exam. Do **NOT** use correction fluid on the exam or on the OMR scan sheet. An answer key will be posted on the course Web site.

OMR Examination Instructions

NOTE: IT IS YOUR RESPONSIBILITY TO ENSURE THAT THE ANSWER SHEET IS PROPERLY COMPLETED: YOUR EXAMINATION RESULT DEPENDS UPON PROPER ATTENTION TO THESE INSTRUCTIONS.

The scanner, which reads the sheets, senses the shaded areas by their nonreflection of light. A heavy mark must be made, completely filling the circular bubble, with an HB pencil. Marks made with a pen or felt-tip marker will **NOT** be sensed. Erasures must be thorough or the scanner may still sense a mark. Do **NOT** use correction fluid on the scan sheet. Do **NOT** put any unnecessary marks or writing on the sheet.

(1) Print your name, student number, course name, section number, and the date in the space provided at the top of SIDE 1 (red side) of the form. The sheet **MUST** be signed in the space marked SIGNATURE.

(2) Mark your student number in the space provided on the sheet on SIDE 1 and **fill in the corresponding bubbles underneath**.

(3) Mark only **ONE** choice from the alternatives (A,B,C,D,E or 1,2,3,4,5) provided for each question. For a True/False question, enter a response of A or 1 for True and B or 2 for False. The question number is to the left of the bubbles. Make sure that the number of the question of the scan sheet is the same as the question number on the exam.

(4) Pay particular attention to the Marking Directions on the form.

(5) Begin answering questions using the first set of bubbles, marked "1".

Continued on page 2

(1) [1 pt.] A TCP segment with the FIN bit set is a request to close both directions of a TCP connection. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(2) [1 pt.] The Open Systems Interconnection Reference Model is composed of five layers. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(3) [1 pt.] Public-key encryption has made conventional encryption obsolete. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(4) [1 pt.] Secure Shell (SSH) uses conventional encryption for authentication. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(5) [1 pt.] The *foundational packet filtering policy* is highly permissive. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(6) [1 pt.] The RSA encryption algorithm exploits the fact that it is many times harder to factor integers than to multiply integers. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(7) [1 pt.] The main weakness of link encryption is that packets travel through routers unencrypted. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

Continued on page 3

(8) [1 pt.] The header of a TCP packet says which process sent the packet and which process is intended to receive the packet. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(9) [1 pt.] An application implemented on top of UDP, like TFTP, may provide reliable communication. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(10) [1 pt.] A server process can listen at a UDP port and a TCP port at the same time. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(11) [1 pt.]. Bluetooth is a public-key encryption algorithm? Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(12) [1 pt.]. The Border Gateway Protocol is used to exchange routing table entries between *autonomous systems*. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

(13) [1 pt.]. The Point-to-Point Tunneling Protocol (PPTP) is used to bypass honeypots. Is this statement true or false?

A.) True.

B.) $\boxed{\text{False.}}$

(14) [1 pt.] The ARP protocol was used on the Little Internet. Is this statement true or false?

A.) $\boxed{\text{True.}}$

B.) False.

Continued on page 4

(15) [2 pts.] Which protocol might give a hacker the means to steal files?

A.) FTP.

B.) HTTP.

C.) NFS.

D.) $\boxed{\text{All of the above.}}$

(16) [2 pts.] A host with one physical network interface running TCP/IP will usually have _____ direct and indirect nonhost routes in its routing table.

A.) 1.

B.) 2.

C.) $\boxed{\text{3.}}$

D.) 4.

(17) [2 pts.] UDP-based services are very difficult to manage with a firewall consisting of just

A.) $\boxed{\text{A standard packet filter.}}$

B.) A stateful packet filter.

C.) A proxy server.

D.) All of the above.

(18) [2 pts.] The idea of public-key encryption was first publicly announced by

A.) National Security Agency (NSA).

B.) $\boxed{\text{Diffie and Hellman.}}$

C.) Rivest, Shamir, and Adleman.

D.) Bruce Schneier.

(19) [2 pts.] The best mechanism for preventing source address spoofing by packets coming from the Internet into a network is

A.) An application-based firewall between the Internet and the network.

B.) A circuit-level gateway between the Internet and the network.

C.) $\boxed{\text{An inbound filter on the network's outermost router.}}$

D.) An outbound filter on a choke router.

Continued on page 5

(20) [2 pts.] Public-key encryption is not especially good for

A.) Creating digital signatures.

B.) $\boxed{\text{Encrypting large amounts of data.}}$

C.) Secret-key exchange.

D.) Protecting the integrity of data.

(21) [2 pts.] Suppose a packet passes through (enters and exits) a computer running `ipfw`. How many filters will it pass through?

A.) 0.

B.) 1.

C.) 2.

D.) $\boxed{3.}$

(22) [2 pts.] The address 243.17.36.1 is a member of

A.) A class A network.

B.) A class B network.

C.) A class C network.

D.) $\boxed{\text{None of the above.}}$

(23) [2 pts.] What is a symptom of the Silly Window Syndrome?

A.) TCP segments receive multiple acknowledgments.

B.) $\boxed{\text{TCP segments carry only a small amount of data.}}$

C.) TCP segments are never acknowledged.

D.) Every TCP segment is duplicated exactly once.

(24) [2 pts.] In the hardware layer of the Internet, messages are encapsulated in

A.) IP datagrams.

B.) UDP datagrams.

C.) TCP segments.

D.) $\boxed{\text{Physical frames.}}$

Continued on page 6

(25) [2 pts.] When the TCP wrapper is running on a host, it controls network access to

A.) All of the host's network servers.

B.) Selected TCP servers.

C.) $\boxed{\text{Selected UDP and TCP servers.}}$

D.) Selected TCP clients and servers.

(26) [2 pts.] A DNS name server listens at

A.) A UDP port.

B.) A TCP port.

C.) $\boxed{\text{Both a UDP port and a TCP port.}}$

D.) A range of UDP ports.

(27) [2 pts.] The TCP protocol can handle

A.) Lost packets.

B.) Duplicated packets.

C.) Out-of-order packets.

D.) $\boxed{\text{All of the above.}}$

(28) [2 pts.] What application protocol uses more than one TCP connection in a session?

A.) Secure shell.

B.) DNS.

C.) $\boxed{\text{FTP.}}$

D.) All of the above.

(29) [2 pts.] The `/etc/inetd.conf` file

A.) Specifies the access control rules for the TCP wrapper.

B.) $\boxed{\text{Maps network services to server programs.}}$

C.) Maps UDP and TCP port numbers to network servers.

D.) Maps network servers to network clients.

Continued on page 7

(30) [2 pts.] The `/etc/ftpusers` file holds the names of the user accounts

A.) That are allowed to use an FTP client.

B.) That are allowed to log into the host's FTP server.

C.) $\boxed{\text{That are not allowed to log into the host's FTP server.}}$

D.) That have ever used the FTP network service.

(31) [2 pts.] In subnet routing, a route has the form (a, m, r, i) where a is a subnet address, m is a subnet mask, r is $*$ or a router's IP address, and i is an interface name. Which IP address matches the route

$$(12.35.46.57,\ 255.128.255.255,\ 34.53.211.2,\ \texttt{eth0})\ ?$$

A.) 12.35.46.0.

B.) 34.53.211.2.

C.) $\boxed{\text{12.42.46.57.}}$

D.) 12.200.46.57.

(32) [2 pts.] What mechanism of TCP is for achieving communication efficiency?

A.) Window advertisement.

B.) Round trip sampling.

C.) Silly window avoidance.

D.) $\boxed{\text{All of the above.}}$

(33) [2 pts.] Which network service is based on ICMP?

A.) DNS.

B.) $\boxed{\text{Ping.}}$

C.) SMTP.

D.) X Windows.

(34) [2 pts.] How are the SYN and ACK bits set in the TCP packet that is used to initiate a TCP connection?

A.) SYN to false, ACK to false.

B.) SYN to false, ACK to true.

C.) $\boxed{\text{SYN to true, ACK to false.}}$

D.) SYN to true, ACK to true.

Continued on page 8

(35) [2 pts.] Which of the following network services is the most dangerous?

A.) Finger.

B.) Rlogin.

C.) $\boxed{\text{TFTP.}}$

D.) Gopher.

(36) [2 pts.] The *transport layer* of the Internet Layering Model is concerned with

A.) Network interface to network interface communication.

B.) Host to host communication.

C.) $\boxed{\text{Process to process communication.}}$

D.) Application to application communication.

(37) [2 pts.] What TCP code bit is used to force data to be sent immediately?

A.) RST.

B.) $\boxed{\text{PSH.}}$

C.) FIN.

D.) SYN.

(38) [2 pts.] The acknowledgement number of a TCP segment is

A.) The sequence number of the last segment received by the segment's sender.

B.) $\boxed{\text{The number of the first octet that has not yet been received by the segment's sender.}}$

C.) The total number of octets that have been received by the segment's sender.

D.) The length of the segment's sender's congestion window.

(39) [2 pts.] Which Unix program can be used to "sniff" the UDP traffic on an Ethernet network?

A.) $\boxed{\texttt{tcpdump}\text{.}}$

B.) `traceroute`.

C.) `udpsniff`.

D.) `ping`.

Continued on page 9

(40) [2 pts.] Which protocol allows circuit-switched communication to be performed over a packet-switched network?

A.) IP.

B.) UDP.

C.) RIP.

D.) $\boxed{\text{TCP.}}$

(41) [2 pts.] Which of the following offers a way of increasing the available set of IP addresses?

A.) IPv6.

B.) Network Address Translation.

C.) Subnet addressing.

D.) $\boxed{\text{All of the above.}}$

(42) [2 pts.] Kerberos tickets are used to

A.) Certify the authenticity of a user.

B.) $\boxed{\text{Grant to a user access rights to a certain service.}}$

C.) Send passwords across a Kerberos-enabled network.

D.) All of the above.

(43) [2 pts.] Do any network servers listen at UDP or TCP ports greater than 1023? If so, give an example of one.

Answer: Yes, an X Windows server listens at TCP port 6000.

(44) [3 pts.] Give an example of a connection-oriented physical network.

Answer: ATM.

(45) [3 pts.] Give an example of how Unix violates the principle of least privilege.

Answer: Unix gives the root user *all* the privileges of a host (including, for example, the privilege to read the mail belonging to other users).

Continued on page 10

(46) [3 pts.] What is dangerous about a Unix file whose owner is `root`, whose group is `nobody`, and whose file permissions are `rws---rwx`?

Answer: This file runs as root when it is executed, it can be executed by any user, and it can be modified by any user. Therefore, any user can use this file to gain any or all root privileges.

(47) [3 pts.] What is the purpose of a portmapper?

Answer: A portmapper is a network server on a host that, given a service S in a request, replies with the protocol (UDP or TCP) and port number of the server that provides S (if the service is offered on the host).

(48) [3 pts.] Why should there be separate disk partitions for the `tmp` and `var` directories?

Answer: A denial of service attack could attempt to fill up either of these directories and thereby prevent a host from functioning by exhausting its disk space. This kind of attack can be thwarted if there are separate disk partitions for these directories.

(49) [3 pts.] For what purpose is public-key encryption often used in applications of conventional encryption?

Answer: Public-key encryption is often used for exchanging secret keys for conventional encryption.

(50) [4 pts.] Name two network services that can be used to probe a network.

Answer: Ping and DNS.

(51) [6 pts.] What is the subnet mask of

A.) A class B network?

Answer: 255.255.0.0.

B.) The subnet consisting of just the IP address 45.56.78.211?

Answer: 255.255.255.255.

C.) The subnet consisting of the IP addresses 11.22.33.0, 11.22.33.1, 11.22.33.2, and 11.22.33.3?

Answer: 255.255.255.252.

The End