Computer Science 3CN3 and Software Engineering 4C03
Final Exam Answer Key

DAY CLASS — Dr. William M. Farmer
DURATION OF EXAMINATION: 2 Hours
MCMASTER UNIVERSITY FINAL EXAMINATION — April 2008

THIS EXAMINATION PAPER INCLUDES 9 PAGES AND 37 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, but you may not use any calculators or other electronic devices. Answers to the first thirty questions (1–30) are to be marked on the OMR scan sheet. Answer the last seven questions (31–37) 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. Good luck!

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) [2 pts.] 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.) [True.]

B.) False.

(2) [2 pts.] A stateful packet filter on a host keeps a record of the packets that it has processed. Is this statement true or false?

A.) [True.]

B.) False.

(3) [2 pts.] A Java applet is an example of mobile code. Is this statement true or false?

A.) [True.]

B.) False.

(4) [2 pts.] On a Unix system a network server can listen at an ephemeral UDP or TCP port. Is this statement true or false?

A.) [True.]

B.) False.

(5) [2 pts.] For SSH with public key authentication, the passphrase is used just like a normal password. Is this statement true or false?

A.) True.

B.) [False.]

(6) [2 pts.] Suppose you are logged into host h and would like to run an X Windows client on a remote host h'. Before this can be done, it is necessary to authenticate the client to the X windows server running on h'. Is this statement true or false?

A.) True.

B.) [False.]

(7) [2 pts.] Today a domain name can be spoofed effectively without spoofing its corresponding source address. Is this statement true or false?

A.) True.

B.) [False.]

Continued on page 3

(8) [2 pts.] Every Ethernet frame contains an IP datagram in its data area. Is this statement true or false?

A.) True.

B.) [False.]

(9) [2 pts.] A host on which an FTP server is running in passive mode cannot be protected by a stateless packet filter. Is this statement true or false?

A.) [True.]

B.) False.

(10) [2 pts.] SSH utilizes public key encryption but not conventional encryption. Is this statement true or false?

A.) True.

B.) [False.]

(11) [2 pts.] The purpose of the `inetd` daemon is to

A.) Broadcast the network services that a host provides.

B.) Give the protocol (UDP or TCP) and port number of the server that provides a requested service.

C.) Filter the network requests received by a host.

D.) [Listen at UDP and TCP ports on behalf of other servers.]

(12) [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.) [SYN to true, ACK to false.]

D.) SYN to true, ACK to true.

(13) [2 pts.] The `ping -R` utility available on the Little Internet traces the route of an IP datagram by exploiting

A.) ICMP time exceeded messages.

B.) ICMP host unreachable messages.

C.) [The record route IP option.]

D.) All of the above.

Continued on page 4

(14) [2 pts.] Suppose h is a host running TCP/IP. h needs to have IP forwarding turned on if

A.) It has more than one physical network interface.

B.) It has a routing table.

C.) It is an *internet router* that connects two physical networks.

D.) All of the above.

(15) [2 pts.] A firewall with a screened subnet architecture usually contains

A.) One or more routers running packet filters.

B.) One or more hosts running proxy servers.

C.) One or more worldwide accessible servers such as a web server.

D.) All of the above.

(16) [2 pts.] Which TCP code bit is a signal to immediately end a TCP connection?

A.) `RST`.

B.) `PSH`.

C.) `URG`.

D.) `FIN`.

(17) [2 pts.] Someone who wants to break into a host will often use port scanning to find

A.) Which ports are currently in use.

B.) All the host's open TCP connections.

C.) The best place to install a virus.

D.) Servers that could be exploited.

(18) [2 pts.] Which kind of server can be extremely dangerous if it is misconfigured?

A.) FTP.

B.) HTTP.

C.) TFTP.

D.) All of the above.

Continued on page 5

(19) [2 pts.] Conventional key encryption is used mostly for

A.) Confidentiality.

B.) Integrity.

C.) Availability.

D.) All of the above.

(20) [2 pts.] Which kind of server is gradually replacing anonymous FTP servers?

A.) SSH servers that offer SFTP.

B.) TFTP servers.

C.) X Windows servers.

D.) HTTP servers.

(21) [2 pts.] Which of the following encryption algorithms is the best for link encryption?

A.) RSA.

B.) DES.

C.) AES.

D.) Diffie-Hellman.

(22) [2 pts.] A security mechanism used by an organization is

A.) A component of the organization's security posture.

B.) A component of the organization's security policy.

C.) A component of the organization's firewall.

D.) All of the above.

(23) [2 pts.] The address 226.127.192.7 is a member of

A.) A class A network.

B.) A class B network.

C.) A class C network.

D.) None of the above.

Continued on page 6

(24) [2 pts.] The *ping of death* is

A.) An ICMP echo request flood that disables a host.

B.) An ICMP echo reply flood that disables a host.

C.) An extremely large ICMP echo request message that disables a host.

D.) A probing of a network using ping that finds a critical weakness in the security of the network.

(25) [2 pts.] Which of the following protocols simultaneously uses more than one TCP connection between a client and a server?

A.) HTTP.

B.) TFTP.

C.) FTP.

D.) All of the above.

(26) [2 pts.] A client process

A.) May directly communicate with other client processes using TCP.

B.) May listen for requests at TCP ports.

C.) May simultaneously participate in more than one TCP connection.

D.) May initiate TCP connections.

(27) [2 pts.] Key management is a major concern for

A.) Conventional encryption.

B.) Public key encryption.

C.) Both conventional and public key encryption.

D.) One-way encryption.

(28) [2 pts.] Public key encryption is not generally suited for

A.) Creating digital signatures.

B.) Protecting the integrity of documents.

C.) Protecting the confidentiality of cryptographic keys.

D.) Protecting the confidentiality of documents.

Continued on page 7

(29) [2 pts.] The *Foundational Packet Filtering Policy* does not allow

A.) An organization's web servers to be accessed from the Internet.

B.) The organization's hosts to access web servers on the Internet.

C.) IP traffic.

D.) All of the above.

(30) [2 pts.] Plato is

A.) A philosopher who argued that physical objects are shadows of their ideal forms which exist in "Platonic heaven".

B.) The founder of the Academy, the longest surviving institution of higher learning in the history of mankind.

C.) The writer of the *Symposium*, a dialogue on the subject of love.

D.) None of the above.

(31) [4 pts.] Explain in a sentence or two why applications that need reliable communication may use UDP instead of TCP.

Answer: The application may need some communication reliability but not all of the reliability provided by TCP. In this case, the overhead cost of using TCP can be avoided by using UDP (which provides no reliability) with some reliability built on top of UDP.

(32) [4 pts.] Why is an Ethernet switch more secure than an Ethernet hub?

Answer: A Ethernet hub forwards an Ethernet frame to *all* the devices to which it is connected, while an Ethernet switch forwards an Ethernet frame, directly or indirectly, only to the hosts that possess the frame's destination address.

(33) [4 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.

(34) [4 pts.] What is the subnet mask of a subnet consisting of the IP addresses 17.19.23.0, 17.19.23.1, . . ., 17.19.23.15.

Answer: 255.255.255.240.

Continued on page 8

(35) Consider a subnet whose subnet address is 16.32.48.64 and whose (unconventional) mask is 255.255.112.112.

A.) [4 pts.] What are the lowest and highest addresses in this subnet?

Answer: 16.32.48.64, 16.32.191.207.

B.) [4 pts.] How many IP addresses are contained in this subnet?

Answer: $2^{5+5} = 2^{10}$.

(36) [4 pts.] Why should a computer with a small disk have separate disk partitions for the `tmp` and `var` directories.

Answer: If a computer with a small disk has only one disk partition, 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.

(37) [12 pts.] Below is a diagram of a conventional internet using the TCP/IP protocols.

THE DIAGRAM IS NOT SHOWN.

$\mathsf{H}_1, \ldots, \mathsf{H}_3$ are hosts. $\mathsf{I}_1, \ldots, \mathsf{I}_7$ are interfaces to the single physical networks $\mathsf{SPN}_1, \ldots, \mathsf{SPN}_5$. $\mathsf{J}_1, \ldots, \mathsf{J}_3$ are interfaces to loopback networks. There are other hosts and interfaces that are not shown. The following table shows what IP addresses and subnet masks are assigned to the $\mathsf{I}_1, \ldots, \mathsf{I}_7$ interfaces.

Interface	IP Address	Subnet Mask
I_1	210.18.183.6	255.255.255.240
I_2	210.18.183.17	255.255.255.240
I_3	210.18.183.18	255.255.255.240
I_4	210.18.183.42	255.255.255.240
I_5	210.18.183.56	255.255.255.240
I_6	210.18.183.58	255.255.255.240
I_7	210.18.183.71	255.255.255.240

Recall that a route in a subnet routing table has the form (a, m, r, i) where:

- a is the address of a subnet S.
- m is the mask of S.
- r is an IP address for the "next hop" ($r = *$ for direct routes).
- i is an interface.

Continued on page 9

Write down an appropriate routing table for H_2 as a list of (a, m, r, i) tuples. *Do not use a default route or any host-specific routes.*

Answer:

(127.0.0.0,	255.0.0.0,	$*$,	J_2)
(210.18.183.16,	255.255.255.240,	$*$,	I_3)
(210.18.183.32,	255.255.255.240,	$*$,	I_4)
(210.18.183.48,	255.255.255.240,	$*$,	I_5)
(210.18.183.0,	255.255.255.240,	210.18.183.17,	I_3)
(210.18.183.64,	255.255.255.240,	210.18.183.58,	I_5)

The End