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 2009

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.] A computation that is *mathematically infeasible* may nevertheless be possible to perform given enough time and space. Is this statement true or false?

A.) [True.]

B.) False.

(2) [2 pts.] Information warfare is an idea that has not yet been used in practice. Is this statement true or false?

A.) True.

B.) [False.]

(3) [2 pts.] A packet filter can catch any packet with a spoofed source address. Is this statement true or false?

A.) True.

B.) [False.]

(4) [2 pts.] Key distribution and management is a major concern for conventional encryption but not for public key encryption. Is this statement true or false?

A.) True.

B.) [False.]

(5) [2 pts.] The underlying principles of today's Internet were developed under funding by the U.S. Department of Defense. Is this statement true or false?

A.) [True.]

B.) False.

(6) [2 pts.] There is no effective defense against the *ping of death*. Is this statement true or false?

A.) True.

B.) [False.]

(7) [2 pts.] Every host running on the Internet has a domain name in the DNS system. Is this statement true or false?

A.) True.

B.) [False.]

Continued on page 3

(8) [2 pts.] According to the TCP protocol, each lost TCP segment will be retransmitted exactly once. Is this statement true or false?

A.) True.

B.) [False.]

(9) [2 pts.] `tcpdump` utilizes the TCP protocol. Is this statement true or false?

A.) True.

B.) [False.]

(10) [2 pts.] The generic top-level domain `gov` is used by the the U.S. government, the U.N., and other national governments. Is this statement true or false?

A.) True.

B.) [False.]

(11) [2 pts.] Which protocol does not use the client-server model?

A.) UDP.

B.) TCP.

C.) [ICMP.]

D.) None of the above.

(12) [2 pts.] A company that strictly enforces the Foundational Packet Filtering Policy using a firewall would allow

A.) Employees inside the firewall to start up X Window clients outside of the firewall.

B.) Employees outside of the firewall to connect to the company's web server.

C.) [Port scanning of the computers inside the firewall from computers from outside of the firewall.]

D.) Computers inside the firewall to be pinged by computers outside the firewall.

(13) [2 pts.] In a normal TCP connection there would be _____ segment(s) with the SYN code bit set to 1, _____ segment(s) with the ACK code bit set to 0, and _____ segment(s) with the FIN code bit set to 1.

A.) 2,2,2.

B.) 3,1,4.

C.) 3,2,2.

D.) 3,2,4.

Note: The correct answer is 2,1,2. Therefore, this is a free question.

Continued on page 4

(14) [2 pts.] Which of the following network protocols is now essentially obsolete?

A.) Gopher.
B.) FTP.
C.) Telnet.
D.) All of the above.

(15) [2 pts.] Which protocol transfers all data as ASCII text?

A.) FTP.
B.) SMTP.
C.) HTTP.
D.) All of the above.

(16) [2 pts.] Which of the following servers is a "meta-server"?

A.) `ftpd`.
B.) `httpd`.
C.) `sshd`.
D.) `inetd`.

(17) [2 pts.] The *need-to-know principle* is a special case of the

A.) Separation of concerns.
B.) Principle of least privilege.
C.) Information hiding.
D.) Plato's notion of perfect forms.

(18) [2 pts.] The SSH protocol uses public key encryption for

A.) Server authentication
B.) Session key exchange.
C.) User authentication.
D.) All of the above.

(19) [2 pts.] What does it mean if `ftp` is in the file `/etc/ftpusers`?

A.) All users have access to the local FTP server.
B.) No users have access to the local FTP server.
C.) Only anonymous users have access to the local FTP server.
D.) No anonymous users have access to the local FTP server.

Continued on page 5

(20) [2 pts.] Suppose it is known that an IP address a has been assigned to some network interface I. Which protocol might be used to find the physical address of I?

A.) Ethernet.

B.) IP.

C.) [ARP.]

D.) DNS.

(21) [2 pts.] An ICMP message would normally be encapsulated in a(n)

A.) Physical frame like an Ethernet frame.

B.) [IP datagram.]

C.) UDP datagram.

D.) TCP segment.

(22) [2 pts.] A session key is

A.) [A conventional encryption key.]

B.) A public key of a public-private key pair.

C.) A private key of a public-private key pair.

D.) A key for one-way encryption.

(23) [2 pts.] Which defense mechanism is adequate for preventing attacks on an anonymous FTP server running in passive mode?

A.) Packet filter.

B.) [Proxy server.]

C.) Screened firewall.

D.) Virtual private network.

(24) [2 pts.] The main purpose of a denial of service attack is to damage _____ of the target of the attack.

A.) Confidentiality.

B.) Integrity.

C.) [Availability.]

D.) All of the above.

Continued on page 6

(25) [2 pts.] To increase security a communication protocol can be tunneled through a(n) _____ communication channel.

A.) IP.
B.) TCP.
C.) [SSH.]
D.) HTTP.

(26) [2 pts.] Which Unix directory is intended for files that can grow arbitrarily large?

A.) `/bin`.
B.) `/etc`.
C.) `/sbin`.
D.) [`/var`.]

(27) [2 pts.] Which protocol uses both UDP and TCP?

A.) FTP.
B.) TFTP.
C.) [DNS.]
D.) HTTP.

(28) [2 pts.] Which of the following encryption algorithms is the best for digital signatures?

A.) [RSA.]
B.) DES.
C.) AES.
D.) Diffie-Hellman.

(29) [2 pts.] Which kind of encryption application is the use of Pretty Good Privacy (PGP) for e-mail?

A.) Link encryption.
B.) [End-to-end encryption at the application layer.]
C.) End-to-end encryption at the transport layer.
D.) End-to-end encryption at the internet layer.

(30) [2 pts.] *Treasure Island* is an adventure novel written by

A.) Rudyard Kipling.
B.) Long John Silver.
C.) Sir Walter Scott.
D.) [Robert Louis Stevenson.]

Continued on page 7

(31) Consider a subnet whose subnet address is 50.100.150.200 and whose (unconventional) mask is 255.170.255.85.

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

Answer: 50.32.150.64, 50.117.150.234.

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

Answer: $2^{4+4} = 2^8$.

(32) [4 pts.] Suppose Mr. A would like to e-mail Ms. B a large binary file. However, Ms. B will accept the file only if she can verify that it has not been modified in transit. How can Mr. A satisfy Ms. B's requirement using public key encryption?

Answer: Mr. A will compute a checksum of the file and then encrypt the checksum with his private key. He will then send Ms. B the file, the encrypted checksum, directions, and possibly his public key. When it arrives, Ms. B will compute a checksum of the file according to the directions, decrypt the checksum with Mr. A's public key, and finally check that the decrypted checksum is identical to the computed checksum. If each step is successful, Ms. B will be justified in assuming that the file has not been modified in transit (provide that the public key is really Mr. A's public key).

(33) [4 pts.] Explain why an Ethernet switch is not an internet router.

Answer: An internet router satisfies the following properties:

1. It is running TCP/IP.
2. It is connected to two or more SPNs via physical network interfaces.
3. Its network interfaces are assigned IP addresses.
4. It can forward incoming IP datagrams to the SPNs to which it is connected.

An Ethernet switch does not satisfy any of these properties.

(34) [4 pts.] Suppose that A, B, and C are hosts on the same SPN with IP addresses a, b, and c, respectively. Suppose further that A routes IP datagrams with destination address c to B and B routes IP datagrams with destination address c to A. What prevents an IP datagram originating at A with destination address c from cycling back and forth forever between A and B?

Answer: The time to live field, which is reduced by one after each hop, will eventually become zero and then the IP datagram will be dropped.

Continued on page 8

(35) [4 pts.] What is the purpose of an X Window server?

Answer: The purpose of an X Window server is to provide display services to X Window clients running locally or remotely. A typical display service is a window on the local computer screen that displays output from the client and returns user input to the client.

(36) [4 pts.] What measures should be taken to prevent a company's web server from being used by intruders as an unintended entranceway to the company's internal network?

Answer: The following measures should be taken:

1. Put the web server on a host that offers no network services except for the services provided by the web server.
2. Make the web server as secure as possible.
3. Make the host as secure as possible, i.e., make it a *bastion host*.
4. Move the host to the company's screened subnet, i.e., put it inside the outer firewall and outside the inner firewall.

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

THE DIAGRAM IS NOT SHOWN.

$\mathsf{H}_1, \ldots, \mathsf{H}_5$ are hosts. $\mathsf{I}_1, \ldots, \mathsf{I}_8$ are interfaces to the single physical networks $\mathsf{SPN}_1, \ldots, \mathsf{SPN}_7$. $\mathsf{J}_1, \ldots, \mathsf{J}_5$ are interfaces to loopback networks. There are other hosts and interfaces that are not named or shown. The following table shows what IP addresses and subnet masks are assigned to the $\mathsf{I}_1, \ldots, \mathsf{I}_8$ interfaces.

Interface	IP Address	Subnet Mask
I_1	237.101.51.35	255.255.255.224
I_2	237.101.51.73	255.255.255.224
I_3	237.101.51.99	255.255.255.224
I_4	237.101.51.91	255.255.255.224
I_5	237.101.51.129	255.255.255.224
I_6	237.101.51.132	255.255.255.224
I_7	237.101.51.133	255.255.255.224
I_8	237.101.51.134	255.255.255.224

Continued on page 9

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.

Write down an appropriate routing table for H_1 as a list of (a, m, r, i) tuples. *The table may include a default route but no host-specific routes.*

Answer:

(127.0.0.0,	255.0.0.0,	$*$,	J_1)
(237.101.51.32,	255.255.255.224,	$*$,	I_1)
(237.101.51.64,	255.255.255.224,	$*$,	I_2)
(237.101.51.96,	255.255.255.224,	$*$,	I_3)
(0.0.0.0,	0.0.0.0,	237.101.51.91,	I_2)

The End