Department of Electrical Engineering and Computer Science
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.033 Computer Systems Engineering: Spring 2000

Handout 30 - Quiz 2

April 14, 2000

All problems on this exam are multiple-choice questions. In order to receive credit you must mark the correct answer or answers for each question. You have 50 minutes to answer this exam.

Write your name on this cover sheet AND at the bottom of each page of this booklet.

Some questions may be much harder than others. Read them all through first and attack them in the order that allows you to make the most progress. *If you find a question ambiguous, be sure to write down any assumptions you make.* Be neat. If we can't understand your answer, we can't give you credit!

THIS IS AN OPEN BOOK, OPEN NOTES QUIZ.

CIRCLE your recitation section number:

10:00	1. Horn/DeCouto	11. Morris/Chao	13. Rudolph/Sit
11:00	2. Horn/Sit	6. Rudolph/Chao	12. Morris/Borodavkina
12:00	5. Poletto/Isla		
1:00	3. Rivest/Tse	7. Saltzer/Isla	8. Poletto/Borodavkina
	10. Balakrishnan/Kaashoek/Chen		
2:00	4. Rivest/Chen	9. Saltzer/Tse	14. Balakrishnan/Kaashoek/DeCouto

Do not write in the boxes below

1-5 (xx/30)	6-9 (xx/24)	10-16 (xx/46)	Total (xx/100)

Name: ______________________________________

I Reading questions

1. [6 points]: Which of the following is true in Mobile IP, as described in the Johnson paper?
(Circle all that apply)

A. A correspondent host can use Mobile IP instead of the address resolution protocol (ARP) to obtain the link-layer address corresponding to the mobile host's IP address.

B. Mobile IP routes packets to a mobile host correctly even if its home agent is a mobile host that has moved away from its home network.

C. Mobile IP provides a way to keep an end-to-end connection alive even if the mobile host moves between different countries.

D. Mobile IP can successfully route packets even if both ends of an end-to-end connection are mobile hosts.

2. [6 points]: Consider the 6.033 protocol reference model with the link, network, and end-to-end layers. Which of the following is a behavior of the reference model?

(Circle all that apply)

A. An end-to-end layer at an end-host tells its network layer which network layer protocol to use to reach a destination.

B. The network layer at a router looks at the end-to-end header and has a separate queue of packets for each end-to-end protocol.

C. The network layer at an end-host looks at the end-to-end type field in the network header and decides which end-to-end layer protocol to invoke.

D. The link layer retransmits packets based on the end-to-end type of the packets: if the end-to-end protocol is reliable, then a link-layer retransmission occurs when a loss is detected at the link layer, otherwise not.

3. [6 points]: Which of the following statements is true about the Click modular router?
(Circle all that apply)

A. During a pull, packets may move backwards through the router graph.

B. Every element contains a queue.

C. Router configurations can be optimized off-line using compiler technology.

D. Every push element must be followed by a push element.

4. [6 points]: Multiple message servers in Grapevine are used to ensure
(Circle all that apply)

A. Scalability.

B. Availability.

C. Performance.

D. Confidentiality.

5. [6 points]: While browsing the Web, you click on a link hosted by an Internet host named `www.lcs.mit.edu`. Your browser asks your Domain Name System (DNS) nameserver, M, to find an IP address for this hostname. Which of the following is **ALWAYS** true of the name resolution process, assuming that all nameservers are configured correctly?
(Circle all that apply)

A. To answer your query, M must ask one of the root nameservers.

B. If M answered a query for `www.lcs.mit.edu` in the past, then it can answer your query without asking any other nameserver.

C. If M has the current IP address of a functioning nameserver for `mit.edu` cached, then that nameserver will be able to directly provide an answer.

D. If M has the current IP address of a functioning nameserver for `lcs.mit.edu` cached, then that nameserver will be able to directly provide an answer.

II A secure Message Transfer Protocol

Ben has studied the pseudo-code implementation of Message Transfer Protocol (MTP) version 1 in Chapter 4 (pages 4-100 through 4-103) with care. This version of the MTP protocol assures message (data) integrity, at-least-once delivery, and delivery accuracy. Throughout the rest of this quiz, the term "MTP" refers to MTP version 1.

For completeness, the pages are included as an appendix to the quiz. Feel free to tear them out so you can refer to them more easily (you don't need to turn them in with your quiz). The questions test high-level knowledge of the pseudocode.

6. [6 points]: MTP tries to assure integrity of
(Circle all that apply)

A. The payload (the `data` field in the `MTP_datagram`).

B. The header (the `MTP_datagram` contents except for the payload).

C. The network layer header.

D. None of the above.

7. [6 points]: MTP assures at-least-once delivery of MTP datagrams under the following conditions
(Circle all that apply)

A. When the network loses messages with low probability.

B. When the network duplicates messages.

C. When the server and listener (the program listening on the MTP port) fail, lose all state, and immediately restart.

D. None of the above.

8. [6 points]: MTP assures at-most-once delivery of MTP datagrams under the following conditions
(Circle all that apply)

A. When the network loses messages with low probability.

B. When the network duplicates messages.

C. When the server and listener (the program listening on the MTP port) fail, lose all state, and immediately restart.

D. None of the above.

9. [6 points]: Why is the `destination` field included in the MTP datagram header?
(Circle the best answer)

A. Because the MTP protocol checks that the network layer routed the datagram correctly.

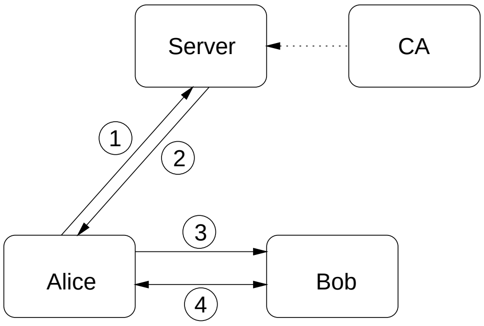
B. Because the end-to-end argument tells us that routing should be performed at the end-to-end layer.

C. Because the network layer uses the MTP datagram header to route the datagram.

D. Because the end-to-end layer at the sender needs it to decide which network protocol to use.

Name: ____

Ben desires message authentication and encryption for data communicated using MTP. He designs a protocol for distributing the keys that will be used for message encryption and authentication. Below is an example of the operation of the protocol, in the case where Alice wishes to communicate securely with Bob:



All messages are communicated using MTP version 1.

1. Alice $\longrightarrow$ Server: "Hi. I am Alice. I want to communicate securely with Bob."
2. Server $\longrightarrow$ Alice: $\{A, K_{A_{pub}}\}_{K_{CA_{priv}}}, \{B, K_{B_{pub}}\}_{K_{CA_{priv}}}$
3. Alice $\longrightarrow$ Bob: $\{\{A, K_{A_{pub}}\}_{K_{CA_{priv}}}, \{B, K_{B_{pub}}\}_{K_{CA_{priv}}}, \{K_{AB}, N\}_{K_{A_{priv}}}\}^{K_{B_{pub}}}$
4. Bob $\longleftrightarrow$ Alice: $\{\text{payload}, N\}^{K_{AB}}$

Conventions:

- CA is a trusted certificate authority. CA is not vulnerable to attack.
- Server (S) is a server that contains certificates provided by the CA. S is vulnerable to attack.
- A is Alice's name; B is Bob's name.
- K_{AB} is a symmetric key; others are public (*pub*) or private (*priv*).
- $\{M\}^K$ denotes message M encrypted with key K.
- $\{M\}_K$ denotes message M signed with key K.
- Step 4 represents multiple messages sent between Alice and Bob.
- N is a nonce chosen by Alice and used in message 3 and all subsequent messages 4.

Name: ____

10. [6 points]: Ben's overall design adheres to the end-to-end argument because
(Circle all that apply)

A. Encryption and authentication are performed at the end nodes instead of at routers.

B. Ben can choose the encryption and authentication ciphers that are most appropriate for Bob, Alice, and the Server without having to modify MTP_send.

C. All programs have to use MTP version 1.

D. All programs have to encrypt and authenticate messages.

11. [6 points]: $\{A, K_{A_{pub}}\}_{K_{CA_{priv}}}$ in message two is an example of
(Circle the best answer)

A. A certificate authority.

B. A signed certificate.

C. A MAC.

D. A symmetric key.

12. [6 points]: What does the nonce in message 4 ensure?
(Circle the best answer)

A. Clock synchronization.

B. Freshness.

C. Confidentiality.

D. None of the above.

13. [6 points]: What do Alice and Bob trust the certificate authority CA to do?
(Circle all that apply)

A. CA has certified that $K_{A_{pub}}$ belongs to Alice.

B. CA has certified that $K_{B_{pub}}$ belongs to Bob.

C. CA keeps $K_{CA_{priv}}$ secret.

D. None of the above.

14. [6 points]: What do Alice and Bob trust the server S to do?
(Circle all that apply)

A. S has certified that $K_{A_{pub}}$ belongs to Alice.

B. S has certified that $K_{B_{pub}}$ belongs to Bob.

C. S keeps $K_{CA_{priv}}$ secret.

D. None of the above.

15. [8 points]: Ben's protocol may be vulnerable to

(Circle all that apply)

A. Impersonation attacks (where Bob can impersonate Alice to a third party), because message 3 doesn't explicitly bind K_{AB} to A and B.

B. Impersonation attacks (where a third party can impersonate Alice to Bob), because message 1 is not encrypted.

C. Replay attacks, because all messages 4 share the same nonce.

D. Known-key attacks, because $K_{A_{pub}}$ is widely known.

16. [8 points]: Lucifer has captured a router on the path between Alice and Bob. He decides to cause mischief by introducing extra MTP ACK packets on the network. Whenever he sees an MTP DATA packet from Alice to Bob, he forwards the packet on to Bob, but also immediately sends Alice an MTP ACK packet for that DATA packet. Assuming this is Lucifer's only form of attack, which of MTP's properties are no longer assured?

(Circle all that apply)

A. Message integrity.

B. At-least-once delivery.

C. Delivery accuracy.

D. All are still assured; extra ACKs will be discarded as duplicates.

End of Quiz 2

Name: ____