

Net ID:

**University of Illinois at Urbana-Champaign  
Department of Computer Science**

Final Exam

CS498SH – Information Assurance

Fall 2006

Monday December 11, 2006

Time Limit: 3 hours

**Instructions for the Student**

Print your name and NetID in the space provided below; **print your NetID in the upper right hand corner of every page.**

Name: \_\_\_\_\_

NetID: \_\_\_\_\_

1. A single page of supplementary notes is allowed
2. Closed book
3. A calculator is allowed.
4. Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
5. Students can use scratch paper if desired.

Number of pages of the exam: 14

Number of questions on the exam: 26

Maximum grade on this exam is: 130 pts

Net ID:

<b>Problem</b>	<b>Points</b>	<b>Score</b>	<b>Grader</b>
1	2		
2	2		
3	2		
4	2		
5	2		
6	2		
7	2		
8	2		
9	2		
10	2		
11	2		
12	2		
13	6		
14	10		
15	9		
16	6		
17	6		
18	10		
19	10		
20	3		
21	8		
22	8		
23	10		
24	4		
25	6		
26	10		

## Information Assurance: Final Exam

### Multiple Choice – 2 points each

1. *Mechanisms used to access resources should not be shared.* This is a definition for which Salzer and Schroeder's Design Principle.
  - a. Principle of Least Privilege
  - b. Principle of Safety
  - c. Principle of Economy of Mechanism
  - d. Principle of Least Common Mechanism
  
2. The Trusted Platform Module (TPM) can create a sealed bound message. What does this involve?
  - a. Encrypt the message with a non-migrateable, public key associated with the target TPM and include PCR values that must be met before the target TPM will decrypt the message.
  - b. Encrypt the message with a non-migrateable, private key associated with the source TPM and include PCR values that must be met before the target TPM will decrypt the message.
  - c. Encrypt the message with a symmetric key shared with the target and source TPM and include PCR values that must be met before the target TPM will decrypt the message.
  - d. Encrypt the message with a non-migrateable, public key associated with the target TPM.
  
3. Which of the following is the best definition of slack space?
  - a. The area of MySpace where the slackers hang out.
  - b. Unused area on the last block of disk assigned to a file.
  - c. Blank pages within a word document.
  - d. Associated streams on the NT File System.
  
4. The Encapsulating Security Payload (ESP) protocol in IPSec allows:
  - a. Encryption but not integrity checks.
  - b. Integrity checks but not encryption.
  - c. Encryption and integrity checks.
  - d. Compression and encryption.
  
5. The legal foundation of our privacy protection is:
  - a. 9<sup>th</sup> amendment
  - b. Communications Assurance for Law Enforcement Act (CALEA)
  - c. 4<sup>th</sup> amendment
  - d. PATRIOT Act

Net ID:

6. Which of the following is the best definition of risk?
  - a. The identification of a weakness in the system.
  - b. Likelihood that an entity will attack the system.
  - c. A board game from Hasbro.
  - d. Probability that a threat will exploit a vulnerability.
  
7. A good encryption algorithm results in cipher text that appears random. Changes to the key are not easily correlated to the cipher text. This property is called:
  - a. Avalanche effect
  - b. Feistel Network
  - c. Pigeonhole principle
  - d. Differential Cryptanalysis
  
8. In Biba's Ring Model, which of the following is true?
  - a. On a read, the subject's level is set to that of the object.
  - b. On a write, the object's level is set to that of the subject.
  - c. On a read, the subject's level is set to the level of the object if the object's level is less than the subject.
  - d. A subject is allowed to read an object only if the object has the same or higher integrity than the subject.
  
9. In which of the following situations is it legal to monitor network traffic?
  - a. Dana hacked into Tara's computer, and Dana is watching Tara's instant message traffic.
  - b. Dana hacked into Tara's computer, and Tara is watching Dana's IRC traffic from the hacked machine.
  - c. Tara is at a coffee shop with unencrypted wireless and is sniffing traffic from Dana's machine.
  - d. Dana and Tara are both logging into a common server owned by the University, and Tara has gained access to observe Dana's instant message traffic from that machine.
  
10. Which of the following is **not** a reasonable protection against online brute force password attack?
  - a. Slowing response after each failed attempt.
  - b. Locking out the account after a fixed number of failed attempts.
  - c. Measure key entry speed to determine whether a human is entering the password, and fail the attempt if the key speed does not what is expected from a human.
  - d. Adding salt to the password.

Net ID:

11. Which of the following is best described as a policy instead of a mechanism?
  - a. Fingerprint readers will be installed at the computing labs.
  - b. Students should be allowed access to the University's computing resources.
  - c. Wireless access points will be installed across the campus.
  - d. Students will be assigned pronounceable, generated passwords once every six months.
  
12. Which of the following is true of the HRU Access Control Matrix model?
  - a. You can prove the safety properties of policies expressed in the model.
  - b. It is an efficient implementation model.
  - c. You can embed many access control policies in the model and compare them on a common footing.







Net ID:

18. (10 points) Imagine that Alice, Bob, Carol, and David have just eaten dinner. The waiter informs them that an anonymous party has paid the bill. One of Alice, Bob, Carol, and David did pay the bill but is too modest to admit it. The diners want to know if one of their party paid the bill, or if the shadowy Eve sitting at the bar did, so they engage in the Dining Cryptographer's protocol. The result of the coin flips is shown below.

<b>Name</b>	<b>Coin Flip</b>	<b>Public Answer</b>	<b>Observed Neighbor</b>
Alice	Head	Different	David
Bob	Head	Same	Alice
Carol	Tail	Different	Bob
David	Tail	Different	Carol

- a) Given the global view of the coin flips, who paid?
  
  
  
  
  
  
  
  
  
  
- b) Select one of the non-payers, and show that that diner cannot guess the identity of the payer with better than uniform probability. Hint: try constructing a table like the one above.



Net ID:

20. (3 points) What are the security fundamentals identified by CIA?

21. (8 points) Identify each security scenario as primarily dealing with C, I, or A.

- a. TotallyThomas shopping web site crashes during the holiday season due to customer overload or extra traffic from DominantlyDiesel.
- b. Customer knows that he is ordering from TotallyThomas.
- c. The TotallyThomas web site provides trustworthy information to its customers.
- d. TotallyThomas protects its cutting edge research from competitors.

Net ID:

22. (8 points) Compare the following labels using the Bell-LaPadula confidentiality policy and indicate what access is allowed: read-only, write-only, both, or none. The levels are: Supreme  $\geq$  High  $\geq$  Normal  $\geq$  Low.

- a. Subject label = Supreme: {A,B} Object Label = Normal: {A}
  
- b. Subject Label = Normal: {A,C} Object Label = High: {B,C}
  
- c. Subject Label = Normal: {A} Object Label = High: {A,B}
  
- d. Subject Label = High: {A} Object Label = High: {A}

23. (10 points) Consider Alice's RSA key pair where  $p = 7$  and  $q = 11$ ,  $e = 17$  and  $d = 53$ .

- a. What is  $n$ ?
  
- b. What is  $\Phi(n)$ ?
  
- c. What is the rule that  $e$  and  $d$  satisfy to be a valid RSA key pair?
  
- d. What is the equation you would solve to encrypt message,  $m$ , to Alice?
  
- e. What is the equation Alice would solve to sign message,  $m$ ?

Net ID:

24. (4 pts) Consider the different modes of AES.

a. List one block-based mode.

b. List one stream-based mode.

25. (6 points) Consider the Vigenere cipher.

a. Use this cipher to encrypt "Bob is good" using the key "Alice". Assume  $a=0$ .

b. Is the Vigenere cipher an example of a:

- i. Substitution cipher
- ii. Transposition cipher,
- iii. Product cipher

Net ID:

26. (10 points) Bert receives the following PGP certificate from Ernie:

Bob(l),Count(h),Maria(l)<<Ernie>>

Where Bob(l) means that Bob signed the certificate with low assurance and Count(h) means Count signed with high assurance.

Bert gathers the following certificates:

Elmo(h),Snuffy(h)<<Count>>

Oscar(h),Snuffy(l)<<Bob>>

In addition, Bert has signed the following certificates himself:

Bert(h)<<Maria>>

Bert(h)<<Elmo>

Bert(l)<<Oscar>>

(a) What are the signature chains that Bert can use to convince himself that Ernie's certificate is trustworthy?

(b) Which chain is the best proof? Why?