

NetID:

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

Midterm 1

CS498SH – Information Assurance

Fall 2006

Wednesday, Sept. 20, 2006

Time Limit: 1 hour and 15 minutes

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: _____

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

Number of pages of the exam: 8

Number of questions on the exam: 13

Maximum grade on this exam is: 72 pts

Problem	Points	Score	Grader
1	2		
2	2		
3	2		
4	2		
5	2		
6	2		
7	2		
8	8		
9	12		
10	12		
11	8		
12	8		
13	10		

Multiple choice (2 points each, 14 total)

1. Which component is **not** a basic component of security as identified by our text.
 - a) Availability
 - b) Confidentiality
 - c) Cryptography
 - d) Integrity

2. What is the name of the principle that says “A subject may not give rights it does not possess to another”
 - a) Principle of Delegation
 - b) Principle of Ownership
 - c) Principle of Safety
 - d) Principle of Attenuation of Privilege

3. Which of the following mechanisms is best described as a mandatory policy?
 - a) The inspector should identify suspicious looking people for more extensive examination.
 - b) Every 10th person in the security line must under go more extensive examination.
 - c) Cars with a single burned out tail light should be pulled over if they are acting otherwise suspicious and you are not otherwise engaged.
 - d) Facebook.com members can select who can access their personal news feed.

4. Which of the following integrity models uses transactions as the basic operation.
 - a) Clark-Wilson
 - b) Lipner's Integrity Matrix
 - c) Biba's Strict Model
 - d) Biba's Ring Model

5. What does law enforcement need to do to legally gain permission for a full content wiretap?
 - a) Prove probable cause to the court.
 - b) Simple request to the court
 - c) Prove probable cause to the FISA court if the subject is not a citizen.

6. In which scenario below is monitoring computer communication or data illegal without court supervision.
 - a) Subject has gained unauthorized access to computer you own.
 - b) You are a service provider, and you need to examine a client's email queue.
 - c) You are playing with a wireless sniffer and testing it out by looking at traffic in the local coffee shop.
 - d) You need to examine an employee's computer, and your company has a policy that makes it clear that content of work computers will be subject to periodic review.

7. Which of the following laws directs the secure operations of many non-governmental companies?
 - a) Federal Information Security Management Act of 2002 (FISMA)
 - b) Clinger-Cohen 1996 or Information Technology Management Reform Act (ITMRA)
 - c) Sarbanes-Oxley Act of 2002 (SOX)
 - d) Carnivore/DCS-1000

NetID:

8. You have been told to come up with mechanisms to implement the following policy.

Employees must eliminate all copies of physical and electronic mail that are more than one year old.

Identify one mechanism that is procedural (i.e. Does not rely on computer automation) and another mechanism that uses computer assistance. (8 points total)

9. (4 points each, 12 total) Consider the set of rights {read (r), write (w), execute(x)} plus copy versions of each right {copy-read(cr), copy-write(cw), copy-execute(cx)}

a) Using the HRU command primitives and conditions, write a command `copy_all_rights(p,q,s)` that copies all rights p has on object s over to q.

b) Modify your `copy_all_rights` command so only the base rights not the copy aspects of the rights are copied.

c) Conceptually, what is the effect of copying the copy flag along with the base right?

10. Perform the access tests between the following labels both as sensitivity labels in the Bell-LaPadula confidentiality model and as integrity labels in the Strict Biba model. For each pair of subject and object labels and each model determine which access is granted of read, write (read also implied), and append (pure write, no read implied). For the levels: Supreme > Good > Maybe > Unknown. (2 points each, 12 total)

- a) Subject=Unknown
Object=Supreme: {A,B,C}
- b) Subject Good: {C}
Object=Good {A,C}
- c) Subject=Supreme: {A}
Object=Maybe: {A,B,C}
- d) Subject=Good: {A,C}
Object=Good: {B,D}
- e) Subject=Unknown: {A}
Object=Unknown: {A}
- f) Subject=Good: {A,B}
Object=Supreme: {A}

11. Recall Biba's low-water-mark policy.

- a) Give a specific example where the integrity levels of the subjects decrease in this model. (4 points)

- b) Under what conditions will the integrity level remain unchanged? (4 points)

12. For each scenario outline a situation where a normal user can cause information to flow counter to the confidentiality assumptions outlined in the Basic Security Theorem. (4 points each, 8 total)

a) A category labeling scheme as implemented in Pitbull LX where reads and writes are allowed if the subject has a superset of categories associated with the object.

b) A Bell-LaPadula implementation that allows a user to have multiple windows open at different security levels

13. A company has been experiencing a rash of laptop thefts. Outline two scenarios driven by different threat-motivations. In each scenario identify (10 points total)
- a) Asset
 - b) Threat-source
 - c) Threat-motivation
 - d) A vulnerability exploited
 - e) A potential control

Scenario 1 (5 points)

Scenario 2 (5 points)