

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

Midterm 1 - Key

CS498SH – Information Assurance

Fall 2006

Wednesday, Sept. 20, 2006

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

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)

There are many possible mechanisms that would satisfy the policy. Here are two examples.

A procedural mechanism: Every month each manager randomly selects an employee, and the manager reviews his computer and physical files for evidence that expired mail has been appropriately deleted.

An automated mechanism: Install a new mail system that enables the automatic expiration of electronic mail files after they have been around for a certain amount of time. The automated approach does not help with physical copies. You could ban printing mail and configure your computers so the print options are disabled to discourage email printing. Or you could invest in hi-tech paper that crumbles after your target period.

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.

Strictly speaking you will need to test for and copy each right. Some folks will no doubt do $A[q,s] = A[p,s]$ which should net partial credit.

I also gave full credit to people who gave the plain right without checking or the copy version.

```
copy_all_rights(p,q,s)
  if cr in A[p,s] and r in A[p,s] then
    enter r in A[q,s]
  if cw in A[p,s] and w in A[p,s] then
    enter w in A[q,s]
  if cx in A[p,s] and x in A[p,s] then
    enter x in A[q,s]
  if rc in A[p,s] then
    enter rc in A[q,s]
  if wc in A[p,s] then
    enter wc in A[q,s]
  if xc in A[p,s] then
    enter xc in A[q,s]
```

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

In this portion, you need to check for the copy right before passing on the regular version

```
copy_all_rights(p,q,s)
  if rc in A[p,s] and r in A[p,s] then
    enter r in A[q,s]
  if wc in A[p,s] and w in A[p,s] then
    enter w in A[q,s]
  if xc in A[p,s] and x in A[p,s] then
    enter x in A[q,s]
```

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

By copying over the copy flag, the original subject loses control over where the right will spread. Beyond delegating the use of the right this enables the target to further delegate the 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}
Supreme: {A,B,C} dominates Unknown: {}
*BLP: append – matches the *-property*
Biba: read – matches the integrity version of the simple security condition
- b) Subject Good: {C}
 Object=Good {A,C}
Good: {A,C} dominates Good: {C}
*BLP: append – matches the *-property*
Biba: read – matches the integrity version of the simple security condition
- c) Subject=Supreme: {A}
 Object=Maybe: {A,B,C}
Supreme: {A} and Maybe: {A,B,C} are incomparable
BLP: none
Biba: none
- d) Subject=Good: {A,C}
 Object=Good: {B,D}
Good: {A,C} and Good: {B,D} are incomparable
BLP: none
Biba: none
- e) Subject=Unknown: {A}
 Object=Unknown: {A}
Unknown: {A} and Unknown: {A} dominate each other
BLP: read, write, append
Biba: read, write, append
- f) Subject=Good: {A,B}
 Object=Supreme: {A}
Good: {A,B} and Supreme: {A} are incomparable
BLP: none
Biba: none

Due to conflicting messages from Jodie and Susan, partial credit was given for F if you were assuming the subject would be changing levels within his clearance to gain access to the Object.

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)

Consider a case where the levels are high > medium > low. The subject is labeled high. The subject reads a file labeled low. By the low-water-mark policy, the read is allowed, but after the read, the subject's label is the minimum of the subject's original label and the object's label, which would be low in this case. Thus, by reading the file labeled low, the subject's label decreases from high to low.

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

If the subject's label is the same or lower than the object's label, the subject's label will be the same after the read operation. Some people also noted that write and execute will not change the subject's label.

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.

The subject has domains (categories) A, B, and C associated. The subject can read a file labeled with A. The subject can then write that information into a file labeled with B.

This breaks assumptions of the basic security theorem. The audience of the information in the first file has increased. Originally only subjects with A label could access the information. After this operation, subjects with the B label will also be able to access the information.

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

Assume the subject has a clearance range of Secret:{A,B,C} – Unclassified. He has one window open at Secret:{A} and another window open at Unclassified:{A}. In the first window he reads information labeled Secret:{A}. In the second window he copies this information into a file labeled Unclassified:{A}. This is obviously declassifying the secret information.

Most (all?) trusted operating systems do not allow cut and paste between windows at different levels. Thus, a user would not be able to accidentally do this. A more dedicated, malicious user could copy down the information he reads in the first window and type it into a file in the second window. But if you have a malicious user with secret clearance, there is probably easier ways to leak the information. But in the typing case, a careless user could get confused and accidentally type sensitive information in the wrong window.

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)

Asset = laptop hardware

Threat-source = cleaning service

Threat-motivation = money

Vulnerability = lack of due diligence in hiring cleaning service or lack of supervision.

Potential control = Installing surveillance cameras, and introducing process that all laptops are taken home or locked in a desk after hours.

Scenario 2 (5 points)

Asset = files on the laptop

Threat-source = competing firm

Threat-motivation = gather information on upcoming product

Vulnerability = company sensitive data stored on laptop, or data is stored in the clear.

Potential control = prohibit company sensitive data from leaving company servers, and require that all laptops have encrypting file systems to store such data.