

Fall 2005 - Information Assurance: Exam 1 answer key

92 points total

1. For each of the items below, is it describing a mechanism or a policy? If it is a policy, describe a possible enforcing mechanism. If it is a mechanism, identify a policy it might be enforcing. (2 pts each, 14 total)
 - a) Employees should be promoted on the basis of the quality of their work in the past year.

This is policy. A mechanism might be procedures to track employee's goals and achievements on a regular basis and use this information in the promotion decision.

- b) Default access for new files set to owner read, write, execute; group read; and no access for other.

This is mechanism. It might be enforcing the policy that default file access should be constrained to the owner and group.

- c) The border firewall drops incoming traffic to the standard HTTP port.

This is mechanism. A possible policy is that company web servers should not be accessible from outside the corporate network.

- d) Incoming students must sign form that confirms they have read the campus acceptable use policy.

This is mechanism. It might be enforcing the policy that all students must be aware of the acceptable use policy.

- e) All employees will ensure that their work computers are secured.

This is policy. An enforcing mechanism might be that IT staff periodically scan the employee machines to detect unsecured machines, and notify the employee to take action.

- f) Employees must maintain an annual trail of work goals for the coming year and reflection on success of previous year's goals.

This is mechanism. It might be enforcing a policy that employees are promoted on merit.

- g) Students can use campus networks for personal email as long as there are sufficient resources for educational purposes.

This is policy. A mechanism might be a tool that drops SMTP traffic when network usage levels reach 80%.

2. Identify the following policies as Discretionary or Mandatory. (1 point each, 5 total)

- a) Every 10th person in the security line must under go more extensive examination.

Mandatory.

- b) Cars with a single burned out tail light should be pulled over if they are acting otherwise suspicious and you are not otherwise engaged.

Discretionary. Policeman gets to use his discretion.

- c) Resource owners should determine who has access to their resources.

Discretionary.

- d) Managers have access to the emails of all direct reports.

Mandatory

- e) Employees can enable family members to access information about company-provided insurance on their behalf.

Discretionary

3. Consider the following scenario. Alice has read and write access to file X and write access to file Y. Bob had read access to file Y and read, write, and execute access to file Z. Carol has read access to files X, Y, and Z.

- a) Write the Access Control Matrix for this scenario (5 points)

	X	Y	Z	Alice	Bob	Carol
Alice	RW	W				
Bob		R	RWX			
Carol	R	R	R			

b) Consider the following command:

```
test_cmd(p, q, s)
    if read in A[p, s] and execute in A[p, s] then
        enter write in A[q, s]
```

With the initial matrix from step a), what is the least number of times this command can be applied before it reaches a state where it will no longer change (i.e., a fixed state). Write the resulting access control matrix. (5 points)

The command can be invoked two times to reach the following state.

Test_cmd(Bob, Alice, Z); Test_cmd(Bob, Carol, Z);

	X	Y	Z	Alice	Bob	Carol
Alice	RW	W	W			
Bob		R	RWX			
Carol	R	R	RW			

4. Compare 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, and append (pure write, no read implied). For the levels: Supreme > Good > Maybe > Unknown. (2 points each, 12 total)

a) Subject=Supreme: {A,B,C}
Object=Unknown

BLP: R Biba: A

b) Subject=Good: {A,C}
Object=Good: {B,D}

BLP: none Biba: none

c) Subject Good: {C}
Object=Good {A,C}

BLP: A Biba: R

d) Subject=Supreme: {A}
Object=Maybe: {A,B,C}

BLP: none Biba: none

- e) Subject=Maybe: {A}
Object=Maybe: {A}

BLP:RWA *Biba:RWA*

- f) Subject=Maybe: {A,B}
Object=Good: {A}

BLP:none *Biba:none*

5. What are the three entities in the *allowed* relationship of the Clark-Wilson model? Briefly describe the relationships between these entities. The enforcement of this relationship was approximated in the Unix system described in class. (5 points total)

Three entities in allowed are:

- *user*
- *transaction procedure*
- *certified data item*

One user, one transaction procedure, and a set of CDI are associated. The user is allowed to invoke the TP on any of the CDI in the set.

6. Describe how the allowed relationship of the Clark-Wilson model helps to enforce two of the five system integrity requirements identified by Lipner. These requirements are listed below for your reference. (6 points total)
1. Users will not write their own programs, but will use existing production programs and databases.
 2. Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
 3. A special process must be followed to install a program from the development system onto the production system.
 4. The special process in requirement 3 must be controlled and audited.
 5. The managers and auditors must have access to both the system state and the system logs that are generated.

Allowed enforces 1 because it ensures that users run only TP's (programs) that someone has set up an allowed relationship for. The normal user cannot set the allowed relation for himself.

Allowed enforces 3 because the installation process must set up the allowed relationships. Since allowed relationships must be set up by administrative users, this will require a special process.

7. When new objects are created in a trusted operating system, it is not immediately clear what the label of the new object should be. Consider the creation of a new file in a MAC file system that follows the Bell-LaPadula model. It could inherit the sensitivity label of the creating process, the enclosing directory, or some combination of the two. Describe two scenarios: one where inheriting the process label makes sense and one where inheriting the directory label might make sense. Consider the implications to confidentiality flow. (10 points)

Scenario 1: The final inherits the process label.

This is essential to ensure confidential information flow is preserved. Any data created by a subject will be created at least at the process label.

Scenario 2: The file inherits the parent directory label.

For process running with multiple categories, it would be more convenient to use the label of the project directory when creating new files. Creating with the process label would make the new data unreadable to others that don't have the same set of categories. However, this breaks confidentiality flow between categories.

8. What are the two major types of risk analysis? Which type is generally used in risk analysis of information systems and why? (4 points)

Quantitative and Qualitative

Qualitative is generally used in the risk analysis of information systems because it is difficult to assign concrete dollar amounts to the results of vulnerabilities and concrete probabilities to the likelihood of a vulnerability being exploited.

9. Several clients of a web hosting company experience web site outages because a disk tray from the web hosting company's server has been stolen. You have been called in to analyze the situation and make recommendations on how this situation can be avoided in the future. Find two scenarios driven by different threat-motivations. In each scenario identify (16 points)
- Asset
 - Threat-source
 - Threat-motivation
 - Two vulnerabilities exploited
 - Two potential controls

Scenario 1:

- Web site data*
- Competing company to the host client*
- Remove site availability so customer's cannot access company critical data (like customer order info)*

- d) 1. Power physical security. 2. Poor new employee verification.
- e) 1. Encrypt data. 2. Better employee checks

Scenario 2:

- a) *Disk drive*
- b) *Disgruntled employee*
- c) *Money*
- d) 1. *Underpaid employee.* 2. *Lack of supervision*
- e) 1. *Pay employee more.* 2. *Install camera*

2. For each situation, under what conditions is the activity legal in the United States? (2 points each, 10 total).

a) Company monitoring employee email.
Notify employee

b) FBI agents monitoring Alice's email conversations with Bob.
Court order with probable cause

c) FBI agents monitoring Alice's email stream to know that she has communicated with Bob.
Court order. Probable cause need not be argued.

d) Carol monitoring Alice's instant messaging communication, where Carol and Alice have no official relationship.
Carol detects communication on Carol's system where Alice is unauthorized.

e) Service provider browsing client's stored email.
Generally allowed. Specified in the company policy.