**CS 370 Introduction to Security Week 6: Problem Set 6**

Instructor Name: Rakesh Bobba

# Introduction / Purpose

The purpose of this assignment is to help you gain a better understanding and insight into role-based and mandatory access control models covered in Week 6.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* Introduction to Role-based Access Control
* Role-Based Access Control Models
* Role Engineering
* Introduction to Mandatory Access Control, Bell-LaPadula (BLP) Model
* Biba Integrity Model
* Chinese Wall Model

Please make sure you read Chapter 8 and Chapter 9 till 9.2.2 from text book

# Instructions/Questions

Please answer the questions below.

## Access Control Concepts

Q1 [2 pts]: What is the difference between a “role” in RBAC and a “group” commonly used in UNIX?

* A role is a collection of permissions. This is contrasted with a group, which is a collection of users.

Q2 [3 pts]: What is separation-of-duty? And what is the difference between static separation-of-duty (SSD) and dynamic separation-of-duty (DSD)

* Separation of Duty is the act of breaking down critical operations such that they require two or more people to complete.
* SSD is the process of using RBAC2 constraints to ensure that two role memberships end up mutually exclusive. This is done by setting a maximal cardinality for a certain user and role set, so that they cannot assume too many (thus conflicting) roles at the same time.
* DSD is another way of resolving conflicts of interest by only letting a user assume n roles of their available role set in a session.

## Role-Based Access Control

Q3 [8 pts]: Consider the following scenario. An organization employs product managers, programmers and testers. The organization operates with the following kinds of files: development code and executables, testing code and executables, test reports, and production code and executables.

Product Managers can view and execute the development executables and production executables to verify correctness. Programmers can create, edit, delete, and execute development code and executables.

Programmers can also promote development code to the test level.

Testers can edit, delete, and execute test code and executables. The testers write test reports that can be read by everyone. The testers can promote test code to production level or demote it back to development.

Everyone can view and execute production code and executables.

Eve is the product manager, Alice and Bob are programmers. Carol and Dave are testers

Would the access control for the scenario above benefit from being implemented in a RBAC system? If yes, explain why and create access matrices that define an RBAC that would enforce this scenario? If not, describe why not and present another scenario that would be better defined as an RBAC system rather than a straight DAC.

* Yes, the above would slightly benefit from RBAC, as there are multiple subjects who are preforming the same jobs or roles (i.e. Alice and Bob are both programmers, so they would both be assigned to the programmer role).

Role Assignments:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Prod. Mgr | Programmer | Tester |
| Eve | X |  |  |
| Alice |  | X |  |
| Bob |  | X |  |
| Carol |  |  | X |
| Dave |  |  | X |

Development code = DC

Development executables = DX

Testing code = TC

Testing executables = TX

Test reports = TR

Production code = PC

Production executables = PX

Permission to Role Mapping

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roles | | | | Files | | | | | | |
|  | PM | Program. | Tester | DC | DX | TC | TX | TR | PC | PX |
| PM | control |  |  |  | [1]  Read  execute |  |  | [5]  Read | [7]  read  execute | [1], [7]  Read  execute |
| Program |  | control |  | [2]  Write  exec.  Delete  read | [2]  Write  exec.  Delete  read | [3]  write |  | [5]  Read | [7]  read  execute | [7]  read  execute |
| Tester |  |  | control | [6]  write |  | [4]  Write  exec.  Delete  read | [4]  Write  exec.  Delete  read | [5]  Write  Delete  read | [6]  write  [7]  read  execute | [7]  read  execute |

[1] Product Managers can view and execute the development executables and production executables to verify correctness.

[2] Programmers can create, edit, delete, and execute development code and executables.

[3] Programmers can also promote development code to the test level.

[4] Testers can edit, delete, and execute test code and executables.

[5] The testers write test reports that can be read by everyone.

[6] The testers can promote test code to production level or demote it back to development.

[7] Everyone can view and execute production code and executables.

Q4 [7 pts]: A company has 20 job functions. On average there are 200 employees in each job function. Similarly, on average an employee in each job function needs 1500 permissions to properly execute their task. Compare the number of assignments that need to be managed i) when using a DAC model vs. ii) when using RBAC model. Generalize the comparison to when the number of job functions is N, number of employees per job function is Ui, where i indexes the job-function, and the number of permissions required per job function is Pi.

## Mandatory Access Control Models

Q5 [4 pts]: What is \*-property in BLP confidentiality model and why is it needed?

Q6 [4 pts]: Compare and contrast BLP and Biba models.

Q7 [2 pts]: What is the difference between a security level and an integrity level?

Q8 [3 pts]: How is Chinese Wall model different from BLP and Biba?

Q9 [6 pts]: When using DAC under MAC in BLP:

* 1. Does a user get access to an object if MAC policy doesn’t permit it? Explain why or why not.
  2. Does a user get access to an object if DAC policy doesn’t permit it? Why or why not.

Q10 [8 pts]: The table below lists subjects, objects, and their associated security levels. The relationship between the levels is as follows: purple > green > orange

|  |  |  |  |
| --- | --- | --- | --- |
| Subject | Subject Clearance | Object | Object Classification |
| Alice | Green | Yoyo | Purple |
| Bob | Purple | XRay | Green |
| Carol | Orange | Zebra | Green |

1. Compute whether the specified subject has read or append (i.e., write but not necessarily

read) access to the specified object (see table below) following the Bell LaPadula model.

|  |  |  |
| --- | --- | --- |
| Subject | Object | Rights |
| Alice | XRay |  |
| Bob | Zebra |  |
| Carol | Yoyo |  |
| Carol | Zebra |  |

b) The security labels are updated to include project categories, p1, p2, and p3. The updated labels are shown in the table below. Re-evaluate the rights (read or append) associated with each subject and object pair following the Bell LaPadula model.

|  |  |  |  |
| --- | --- | --- | --- |
| Subject | Subject Clearance | Object | Object Classification |
| Alice | Green:{p1,p2} | Yoyo | Purple:{p1} |
| Bob | Purple:{p2} | XRay | Green:{p1, p2} |
| Carol | Orange: {p1, p3} | Zebra | Green: {p3} |

|  |  |  |
| --- | --- | --- |
| Subject | Object | Rights |
| Alice | XRay |  |
| Bob | Zebra |  |
| Carol | Yoyo |  |
| Carol | Zebra |  |

Q11 [8 pts]: The table below lists subjects, objects, and their associated ***integrity*** levels. The relationship between the levels is as follows: purple > green > orange

|  |  |  |  |
| --- | --- | --- | --- |
| Subject | Subject Level | Object | Object Level |
| Alice | Green | Yoyo | Purple |
| Bob | Purple | XRay | Green |
| Carol | Orange | Zebra | Green |

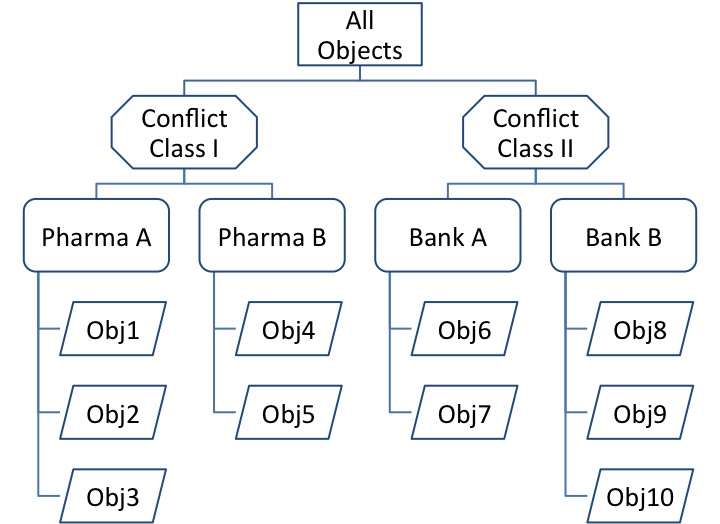
1. Compute whether the specified subject has ***observe (read)*** or ***modify (append or update)*** access to the specified object (see table below) following the ***Biba Strict Integrity Policy***.

|  |  |  |
| --- | --- | --- |
| Subject | Object | Rights |
| Alice | XRay |  |
| Bob | Zebra |  |
| Carol | Yoyo |  |
| Carol | Zebra |  |

1. The ***integrity*** labels are updated to include project categories, p1, p2, and p3. The updated labels are shown in the table below. Re-evaluate the rights (modify or observe) associated with each subject and object pair following the Biba model.

|  |  |  |  |
| --- | --- | --- | --- |
| Subject | Subject Class | Object | Object Class |
| Alice | Green:{p1,p2} | Yoyo | Purple:{p1} |
| Bob | Purple:{p2} | XRay | Green:{p1, p2} |
| Carol | Orange: {p1, p3} | Zebra | Green: {p3} |

|  |  |  |
| --- | --- | --- |
| Subject | Object | Rights |
| Alice | XRay |  |
| Bob | Zebra |  |
| Carol | Yoyo |  |
| Carol | Zebra |  |



Q12 [5 pts]: Figure above depicts organization of objects into datasets (e.g., Bank A) and conflict of interest classes (e.g., Conflict Class I) at consulting firm ConFirm X that uses Chinese Wall access model. Jane, Bob, Emily, Marcus, and Alice are consultants with the firm. Assume that the consultants currently have no other accesses than those explicitly stated. Please answer the following with respect to the above figure when using a Chinese Wall access model.

1. Can Bob be allowed to read Obj 6 and Obj2? Explain why or why not.
2. Can Jane be allowed to read Obj7 and Obj10? Explain why or why not.
3. Can Emily be allowed to read Obj1 and write to Obj9? Explain why or why not.
4. Can Marcus be given read and write access to Obj8 and write access to Obj10? Explain why or why not.
5. Can Alice be given read and write access to Obj6 and Obj 3? Explain why or why not.

# Submission Details

Submit a PDF file with the questions and your corresponding answers

The assignment is worth 60 points. It is due Wednesday of Week 7 at Midnight.