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?

- The difference between a “role” and a “group” is the focus of the term. A “role” is a named job function within an organization, and a user can only fill one role at a time. This allows the user to be given permissions based on their job. A “group” however is a collection of users that are given permissions based on the group they belong to. A group is mainly used when specific people need specific permissions, while a role is used when the administrator wants to set the permissions for the role and then just assign people to the role and not have to worry about permissions later.

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 requiring more than one entity to be present to complete a task. The difference between SSD and DSD is when permission constraints are enforced: SSD enforces at assignment of roles of users, while DSD enforces within the current 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, this would benefit from being implemented in RBAC. This is because each role is clearly defined above and each employee is clearly placed into a role.

Role	Permissions	Members
Product Managers	View{dev exes, prod exes, prod code, test reports} Execute{dev exes, prod exes}	Eve
Programmers	View{prod code, prod exes, test reports} Create{dev code, dev exes} Edit{dev code, dev exes} Delete{dev code, dev exes} Execute{dev code, dev exes, prod exes} Promote{dev code}	Alice Bob

Testers	View{prod code, prod exes, test reports} Edit{test code, test exes, test reports} Delete{test code, test exes} Execute{test code, test exes, prod} Promote/Demote{test code}	Carol Dave

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 U_i, where i indexes the job-function, and the number of permissions required per job function is P_i.

- I) DAC: $N(U_i(P_i))$
- In DAC, each employee has their permissions set individually, so
    - 20 Job functions * 200 employees per function * 1500 permissions per employee.

- Ii) RBAC: $N(P_i) + N(U_i)$

- In RBAC, each job function has its permissions set, then each employee is just added to the role

    - 20 job functions * 1500 permissions per job function + 20 functions * 200 employees per function.

Mandatory Access Control Models

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

- The *-Property is “No Write Down.” This means a subject can only read and write to an object with the same security level and can only append to an object of greater or equal security level.

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

- BLP and Biba differ in their focus: Biba focuses on integrity, while BLP focuses on confidentiality.
- BLP and Biba are similar in that they control who can access which object/asset. Their difference is in approach and focus.

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

- A security level is a label put on an asset/object that ensures subjects without the correct clearance cannot access it e.g. object classified secret; subject with top secret clearance can access object, but subject with below secret clearance can not access object.
- An integrity level is a level of confidence in the asset or object. The higher the integrity level, the higher the confidence is that the program will execute correctly/data is accurate/data is reliable, etc.

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

- Chinese Wall Model differs from BLP and Biba in that it is concerned with conflicts of interest, rather than an object's security or integrity level.

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

a) Does a user get access to an object if MAC policy doesn't permit it? Explain why or why not.
- No, because MAC gives users access privileges based on the group or role they belong to.

b) Does a user get access to an object if DAC policy doesn't permit it? Why or why not.
- Yes, because MAC gives users access privileges based on their group or role privileges, even if the owner of the file doesn't permit access.

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

a) 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	Read
Bob	Zebra	Read
Carol	Yoyo	Append
Carol	Zebra	append

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	Read{p1, p2}
Bob	Zebra	None
Carol	Yoyo	Append{p1}
Carol	Zebra	Append{p3}

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

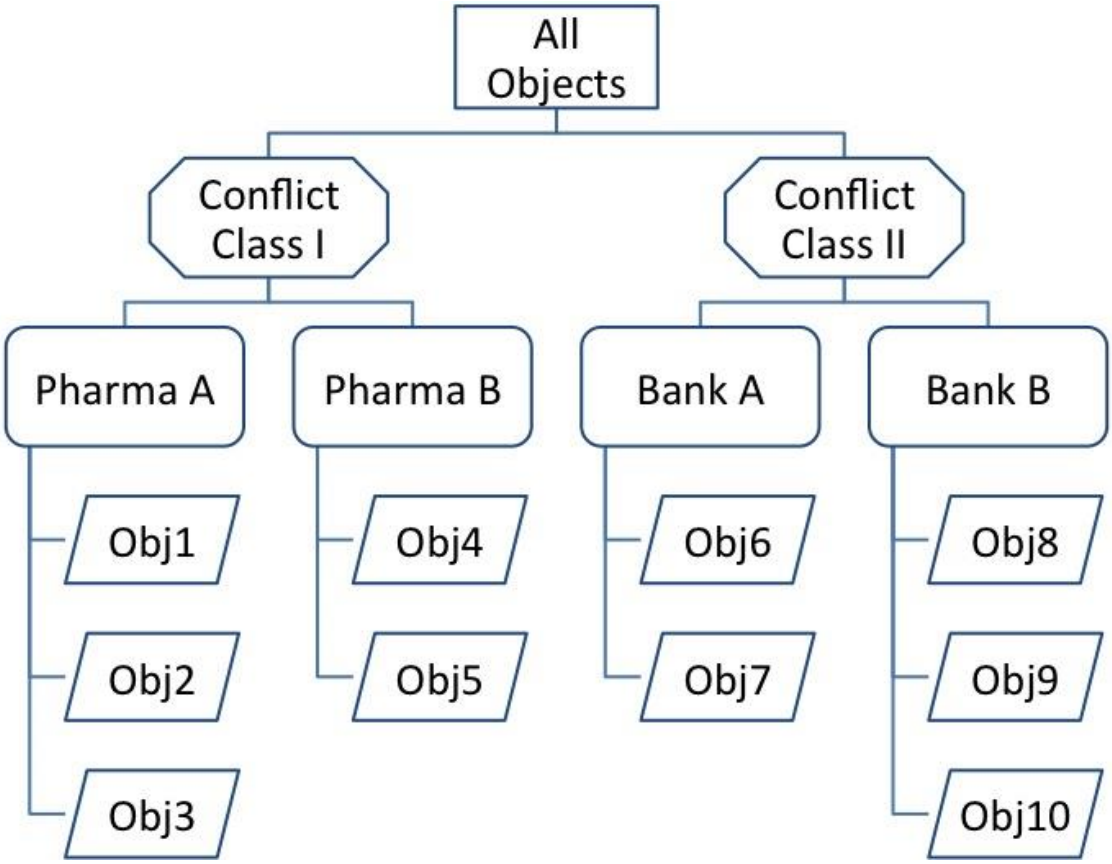
b) Compute whether the specified subject has ***observe (read)*** or ***modify (append or update)*** access to the specified object (see table below) following the ***Biba Strict Integrity Policy***.

Subject	Object	Rights
Alice	XRay	Observe + modify
Bob	Zebra	Modify
Carol	Yoyo	Observe
Carol	Zebra	Observe

c) 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	Observe + modify{p1, p2}
Bob	Zebra	None
Carol	Yoyo	Observe{p1}
Carol	Zebra	Observe{p3}



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.

a) Can Bob be allowed to read Obj 6 and Obj2? Explain why or why not.
   - Yes, because Obj 6 and Obj 2 are within different Conflict Classes. This follows the simple security rule.

b) Can Jane be allowed to read Obj7 and Obj10? Explain why or why not.
   - No, because Obj 7 and Obj 10 are within different Data Sets. This violates the simple security rule.

c) Can Emily be allowed to read Obj1 and write to Obj9? Explain why or why not.
   - No, because Obj 1 and Obj 9 are in different Data Sets. This violates the simple security rule and the star-property rule.

d) Can Marcus be given read and write access to Obj8 and write access to Obj10? Explain why or why not.
   - Yes, because Obj 8 and Obj 10 are in the same Data Set and same Conflict Class. This follows both the simple security rule and the star-property rule.

e) Can Alice be given read and write access to Obj6 and Obj 3? Explain why or why not.
   - No, because Obj 6 and Obj 3 are in different Conflict Classes as well as different data sets. This violates both the simple security rule and the star-property rule.

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.