CS 370 Introduction to Security **Week 5: Problem Set 5**
Instructor Name: Rakesh Bobba

Introduction

The purpose of this assignment is to help you gain a better understanding and insight into access control concepts covered in Week 5.

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

- Introducing Access Control
- Access Control Matrix: An Abstraction
- Changing Access Policy
- Discretionary Access Control in Practice

Please make sure you read Chapter 4 of the textbook, up to section 4.2.7

Questions

Please answer the questions below.

Access Control Concepts

Q1[6 pts]: State and define the three most important components in access control, all starting with the letter ‘A’?

- Authentication: the act of binding an external entity to a system entity.
- Authorization: granting access to a resource.
- Auditing: Independently reviewing system actions

Q2 [4 pts]: What is the primary difference between DAC and MAC access model?

- DAC uses user identifiers whereas MAC uses ‘privilege’ identifiers (i.e. labels).
- DAC allows the user to change the policy, while MAC does not.

Q3 [4pts]: In access control, what does an “open policy” and “closed policy” mean?

- An open policy relates to allowing access to all that are not denied access, i.e. blacklisting.
- A closed policy is the opposite, whereupon only people granted access explicitly can get access.

Q4 [4 pts]: Explain the difference between Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)

- Where RBAC only considers a role or roles that a user is given, ABAC considers the attributes of the person as well as the context of the access when performing authorization.

Access Control Matrix

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

Q5 [3 pts]: Define the rights the access control system would need to enforce the requirements for this scenario. Associate an abbreviation that you can use in the following questions.

- To grant the accesses to these file types, the access control system would need read (r), write (w) and execute (x) on all files that it might be passing out permissions for. Therefor that means:
  - Dev Code: rwx
  - Testing Code: rwx
  - Test Reports: rw
  - Prod Code: rwx

Q6 [7 pts]: Design an access control matrix for the scenario above for the users mentioned.

- The three digits associated with each cell represent r(1|0)w(1|0)x(1|0). 111 represents read, write, execute.
- Promotion and demotion is counted as a write in the target category.
- No execute has been given to code, as the corresponding executable contains those permissions.

	Dev Code	Dev Exe	Test Code	Test Exe	Test Reports	Prod Code	Prod Exe
P. M.		101			100	100	101
Programmer	110	111	110		100	100	101
Tester	110		110	111	110	110	101

Q7 [3 pts]: Assume the Access Matrix is being implemented by a system using Access Control Lists. Write the Access Control List for the Development Executables.

- Dev Executables can be read and executed by the project manager, and can be read, written to and executed by programmers.

Q8 [3 pts]: Assume the Access Matrix is being implemented by a Capability system. Write the Capability list for Alice.

- Alice, being a programmer can read and write development code, and can read, write and execute development executables. They can read and write to test code (by promoting it; write alone would make no sense…). They can read test reports and production code, and can read and run production executables.

Changing Access Control Policy/Matrix

	File 1	File 2	File 3	File 4	Subject A	Subject B	Subject C
Subject A	Own R W		Own R W		Control		Own
Subject B	R	Own R W	W	R*		Control	
Subject C	R W	R		Own R W			Control

Q9 [4 pts]: Keeping in mind the rules governing access control matrix change covered in class, and the access matrix shown above, answer whether or not the following changes to access matrix are allowed. **Explain in one sentence why or why not**.

a) (allowed / **not allowed**) Subject C wants to Transfer R on File 2 to Subject A
    a. Not allowed because SC does not have the "*" on R for File 2
b) (allowed / **not allowed**) Subject A wants to Delete R on File 2 from Subject C
    a. Not allowed, as SA does not have any permissions at all on File 2.

UNIX Permissions

Q10 [5 pts]: When a file in Unix is protected with mode "644" = rw- r-- r-- and is inside a directory with mode "730" = rwx -wx --- can you describe a way in which the file can be compromised?

- Intrigued by how this would be exploited, I set it up on my machine -

```
drwx-wx---  2 root  lread 4.0K Nov  2 05:10 temp/
```

within that directory is a file containing jibberish. The way that this can be exploited is if the attacker and the directory/file share a group in common. For example, I, lread, have group write and execute on the directory, but read access to the file inside. Therefore, if I know the filename, I can cat the file without being able to ‘ls’ the directory, something I imagine the person who set the directory up designed the permissions to prevent me from running.

```
▶ cat temp/test
  jkasdjflkads
```

Q11 [2 pts]: Suppose you are working as the security administrator at xyz.com. You set permissions on a file object in a network operating system which uses DAC (Discretionary Access Control). The Extended ACL (Access Control List) of the file is as follows:
Owner: Read, Write, Execute
User C: Read, Write, -
User B: Read, Write, Execute
Sales: Read, -, -
Marketing: -, Write, -
Mask: Read, Write, -
Other: Read, Write, -

User "A" is the owner of the file. User "B" is a member of the Sales group. What effective permissions does User "B" have on the file?

- User B will have rwx on that file, as their user permissions take precedence over their group permissions.

Submission Details

Submit a PDF file with the questions and your corresponding answers
The assignment is worth 45 points. It is due Wednesday of Week 6 at Midnight.