UNIVERSITY OF MISSOURI-KANSAS CITY

Information Security and Assurance
Assignment - 4

Submitted by:

Anusha Malineni

16233382

Biba Integrity Model:

This is a policy which is developed by Kenneth J. Biba in 1975 to ensure data integrity. This model describes a set of access control rules. This model has different groups of access modes such as execute, invoke, modify, observe. Furthermore, Biba model is divided into two types. They are

- **Mandatory Access Control**
    1. Strict Integrity Policy
    2. Low-water-mark policy for subjects
    3. Low-water-mark policy for objects
    4. Audit policy
    5. Ring Policy
- **Discretionary Access Control**
    1. Access control lists
    2. Object Hierarchy
    3. Ring

Mandatory Access Control:

Let's consider a use case of making and producing a movie which describes all the above policies for better understanding

Subject (S)	Level of Confidentiality		Object (O)	Level of Integrity
Director	H: High		Story Line	H
Producer	MH: Medium High		Production Cost	MH
Main Characters	ML: Medium Low		Lyrics, Composition of Songs etc.	ML
Other members of the team	L: Low		Shooting Spot, Accessories etc.	L

Apart from the story line of the movie, the integrity of making and production also makes any movie a huge success.

1. **Strict Integrity Policy:**

   According to this policy, no write-up and no read-down is restricted i.e., an object cannot be modified by a subject whose integrity is greater than the subject (No Write-Up) and an object cannot be observed by a subject whose integrity level is low than the subject (No Read-Down) respectively. A subject with high confidentiality level can invoke any subject with low confidentiality levels than that.

   Simple: Director of the movie shouldn't have concerns regarding the budget of the movie. Knowing the budget will limit his creativity.

   Star: The story should be written only by the director and not by any members of the team since it might the change the soul of the movie.

   Invoke: The director of the movie can invoke any other person in the team to work.

2. **Low Water-Mark Policy for Subjects:**

   According to this policy, if a subject with high integrity level would like to observe a object with low integrity then the integrity level of the subject will come down to the integrity level of the object.

   Simple: A producer can make false assumptions about the budget related to shooting locations and other accessories required for the making of the movie.

   Star: The story should be written only by the director and not by any members of the team since it might the change the soul of the movie.

   Invoke: The director of the movie can invoke any other person in the team to work.

3. Low Water-Mark Policy for Objects:

According to this policy, any subject can modify any object but the integrity of the subject is low than the integrity level of the object, then the integrity level of the object will come down to the integrity of the level of the subject.

Star: If any of the main characters change the story line of the movie then the integrity level will come down and will be given lesser importance.

4. Audit Policy:

According to this policy, an action must be recorded in the audit logs if a lower integrity level subject modifies an object with higher integrity level than the subject.

Star: If the story line is changed by any other person other than the director, then it should be logged in audit log file. Then the director will review the changes and can add or delete the changes according to his interest.

5. Ring Policy:

According to this policy, any subject can read from any other object. Star and Invoke policies are similar to Strict Integrity Policy.

Simple: The director can view the production cost and can limit the story if it is exceeding the cost.

Star: The story should be written only by the director and not by any members of the team since it might the change the soul of the movie.

Invoke: The director of the movie can invoke any other person in the team to work.

Discretionary Access Control:

1. **Access Control Lists:**

   These lists are used to determine which subjects can access which objects. These lists can be modified with subjects with correct privileges.

   Other guests can login into our personal computer and can access minimal information but only the admin have rights over complete information.

2. **Object Hierarchy:**

   This contains a root and objects which are ancestors to the root. A subject must observe the privileges of an object and all other objects until root to access a particular object.

   An employee in an organization can observe the details of other employees who belong to the same hierarchy in the organization.

3. **Ring:**

   The rings in the system are numbered in this policy where the low numbers have higher privilege. The access mode of the subject should fall within the specific range to get accessed to an object.

   Patients in a hospital are treated by the doctor according to their serial number.