UMKC

Spring-2017

Information Security and Assurance
Assignment-4

Submitted by:

Moulika Chadalavada

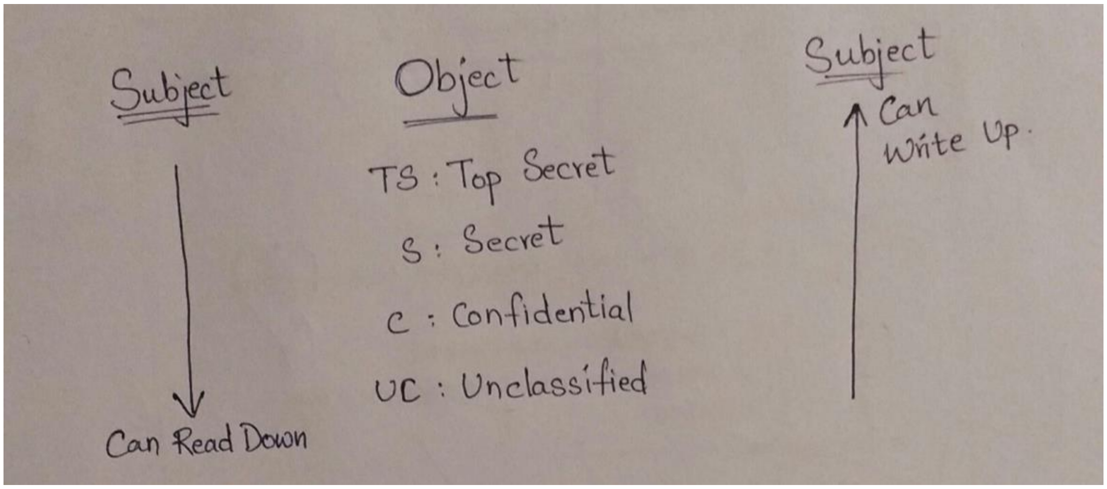
16234180

1. Explain Bella-Padulla model with an example. (1 point)

Answer:

Bell-La Padula is a security policy model developed for implementing security policies. This model focuses on data confidentiality. Sets up security policies between set of objects (O) and subjects (S). Subject is a user who performs operations on objects. Object is an item on which subject performs operation. This model is developed for army to maintain security policies. Subject has security clearance and object has security classification.

Bell-La Padula Model task is to combine security clearance and security classification, to do so model defines some properties they as Star Property, Simple Property, Tranquility Property.



Top Secret > Secret > Confidential > Unclassified

1. **Star Property:** This property is also called as confinement property, which states that subject S can write object O if and only if security clearance of S is lower than or equal to security classification of O, i.e. $I_{sc}(S) \le I_{scl}(O)$. (**No Write Down)**

   Example: A person cannot add SSN information or any other medical information on unclassified websites

2. **Simple Property:** This property states that subject S can read from Object O if and only if Security clearance of S is higher than or equal to security classification of O, i.e. $I_{sc}(S) \ge I_{scl}(O)$. (**No Read Up**).

   Example: First grade students cannot read a book about thermodynamics because it is above their level of vocabulary and comprehension

3. **Tranquility Property:** This property states that security classification of Object O cannot be changed while it is being processed. It has two forms Principle of strong tranquility and Principle of weak tranquility. In Principle of strong tranquility security level don't change during normal operation and in Principle of weak tranquility security levels may never change, but level may be changed when necessary action needs to be completed.

2. Explain Biba mandatory and discretionary policies with examples. (3 points)

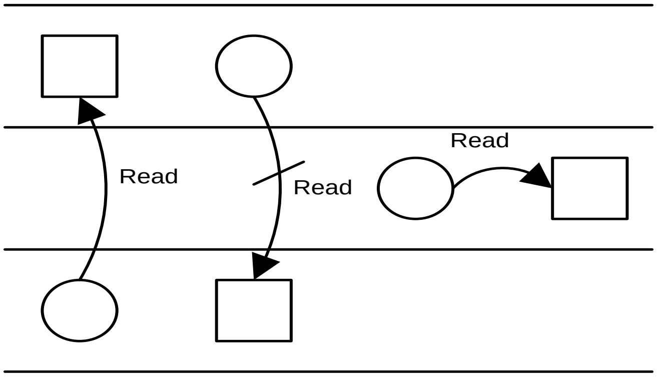
Answer:

Biba Integrity Model is developed by K. Biba to satisfy Information Integrity. It captures integrity aspects of access control. Integrity prevent unauthorized information. Biba Model has group of access modes such as Modify, Observe, Invoke, Execute. Biba Model is divided into two types of policies, they are **mandatory (MAC)** and **discretionary (DAC).** As Bella-Padulla Biba Model also deals with subject and objects and each of them is assigned to integrity level. i(s) -> Integrity level of Subject and i(o) -> Integrity level of object.

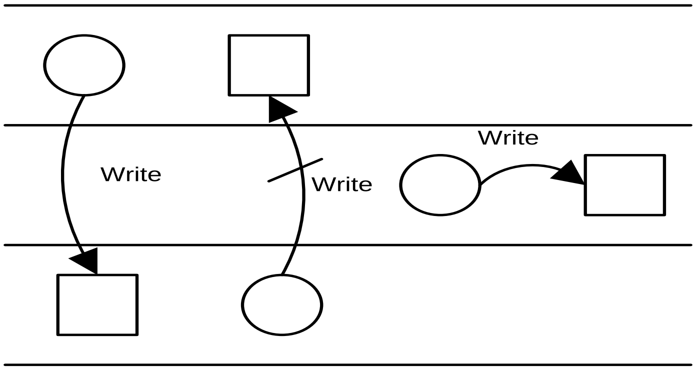
Biba Mandatory Policies:

Below are Biba Mandatory Policies:

1. **Strict Integrity Policy:** This policy enforces no write-up and no write-down. This policy restricts data contamination at higher level as subject is allowed to modify data at its lower level. No write-up limits the damage that is done by Trojan Horse in system. This policy in turn states 3 properties such as
   i. **Simple Integrity Condition:** S can observe O if and only if $i(s) \leq i(o)$
   ii. **Integrity Star Property:** S can modify O if and only if $i(o) \leq i(s)$
   iii. **Invocation Property:** Subject s1 can invoke subject s2 id s2 has lower or equal integrity than s1.



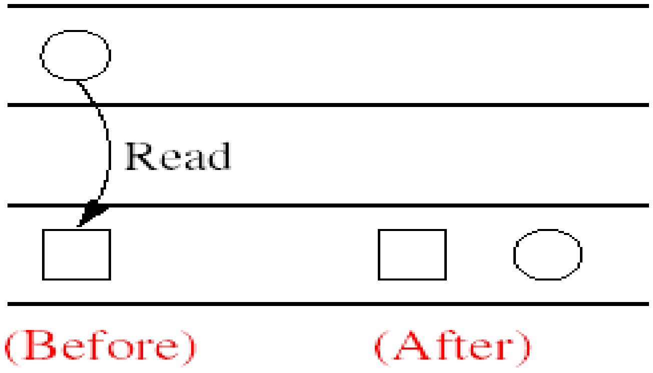
No Read Down



No Write Up

Example: An employee cannot edit manager information who is at higher level. Manger cannot read payslips of employee who are at low level.

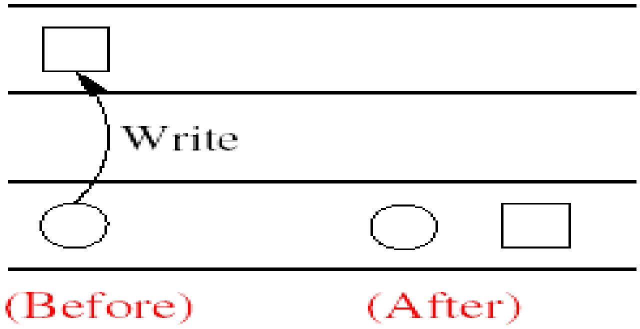
2. **Low-Water-Mark Policy for Subjects:** This policy determines no write up. It states that i'(s) = min(i(s),i(o)) that means if subject S reads less trusted object O then level of S will drop to that of O, which prevent O from contaminating S. This helps in preventing modifying more trusted Os.



circle = subject, square = object

Example: If a machine installs software with virus, then the system will no longer be trusted.

3. **Low-Water-Mark policy for Objects:** This policy lowers integrity level of subject based on observation of Os. It uses invocation property.



circle = subject, square = object

Example: Once virus is installed in system, further whatever files downloaded by virus is not trusted and are deleted to reduce risk.

4. **Low-Water-Mark Integrity Audit Policy:** This policy states that any subject can modify any object irrespective of its integrity levels. If S modifies an O with high integrity level, its transaction is recorded in audit log. The drawback to this policy is that it does nothing to prevent an improper modification of an object to occur

5. **Ring Policy:** In this policy, any subject can observer any object irrespective of its integrity level. It holds Integrity Star and Invocation property.
   Example: A user reading a less trusted object, then remembers the data they read and then, at a later time, writing that data to an object at their integrity level, indirect modification of trusted data

Biba Discretionary Policies:

Below are Biba Discretionary Policies:

1. **Access Control Lists:** Determine which Ss can access which Os. The list can be modified by Ss with correct privileges.
   Example: In our personal laptop guests can login and access minimal information but admin can edit information.

2. **Object Hierarchy:** This method contains root and Os (ancestors to root). To access particular O, S must first observe privileges of O and all other Os till root.
   Example: In an organization employee E_1 can observe details of other employees who also belong to same hierarchy as of E_1.

3. **Ring:** In this method, the rings in the system is numbered, with lower number having higher privilege. The access mode of S should fall within specific range to get permission to access an O.
   Example: Students are allowed to enroll to Spring semester based on GPA.