DBMS

Seminar

Topic: MAC Model

Branch: CSE

Section: A

Group Members:

1. Bhaskar Jyoti Deka(180310007014)

2. Amartya Biswas(180310007006)

3. Darshana Bhuyan(180310007020)

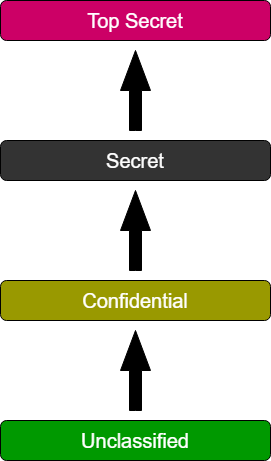
MAC Model

**Definition:** MAC was developed using a nondiscretionary model, in which people are granted access based on information clearance. MAC secures information by assigning sensitivity labels on information and comparing this to the level of sensitivity a user is operating at. MAC access control mechanisms are more secure than DAC yet have trade-offs in performance and convenience to users. MAC mechanisms assign a security level to all information, assign a security clearance to each user, and ensure that all users only have access to that data for which they have a clearance. It is a policy in which access rights are assigned based on central authority regulations. Users cannot change access rights. Example of MAC occurs in military security records, patients medical records, driver records etc.

**Explanation:** Memory access control mechanism can be explained as object(Eg: tables,views and rows), subjects(Eg: users,programs), security classes and clearances. Each database object is assigned to a security class, which define its security parameters and each subject is assigned clearance of security class. A given data object can then be accessed only by users with the appropriate clearance of a particular classification level. Thus, a mandatory access control technique classifies data and users based on security classes such as top secret(TS),secret(S),confidential etc.

**Diagram:**

There are four types of security classification levels:Top Secret (TS), Secret (S), Confidential (C), and Unclassified (U) ,where TS is the highest level and U is the lowest level.

****

**Advantages:**

* High level of data protection - An administrator defines access to objects, and users can’t edit that access.
* Granular - An administrator sets user access rights and object access parameters manually.
* Immune to Trojan Horse attacks - Users can’t declassify data or share access to classified data.
* MAC provides tighter security because only a system administrator may access or alter controls.
* MAC policies reduce security errors.
* MAC enforced operating systems (OS) delineate and label incoming application data, which creates a specialized external application access control policy.

**Disadvantages:**

* Maintainability - Manual configuration of security levels and clearances requires constant attention from administrators.
* Scalability - MAC doesn’t scale automatically.
* Not user friendly - Users have to request access to each new piece of data. They can’t configure access parameters for their own data.
* Lack of flexibility.
* Difficulty in implementing and programming.

**Importance of access control:**

* AC regulates which users, applications, and devices can view, edit, add, and delete resources in an organization’s environment. Controlling access is one of the key practices to protect sensitive data from theft, misuse, abuse, and any other threats. There are two levels of access control: physical and logical.
* Access control helps to mitigate both insider and outsider threats.

**Common MAC models:**

Common MACs models includes Bell-La Padula , Biba, Clark-Wilson.