Do not write in this Margin

UNIVERSITY OF BENIN

Question.....

Write on both side of the paper

39683

Do not write in this Margin

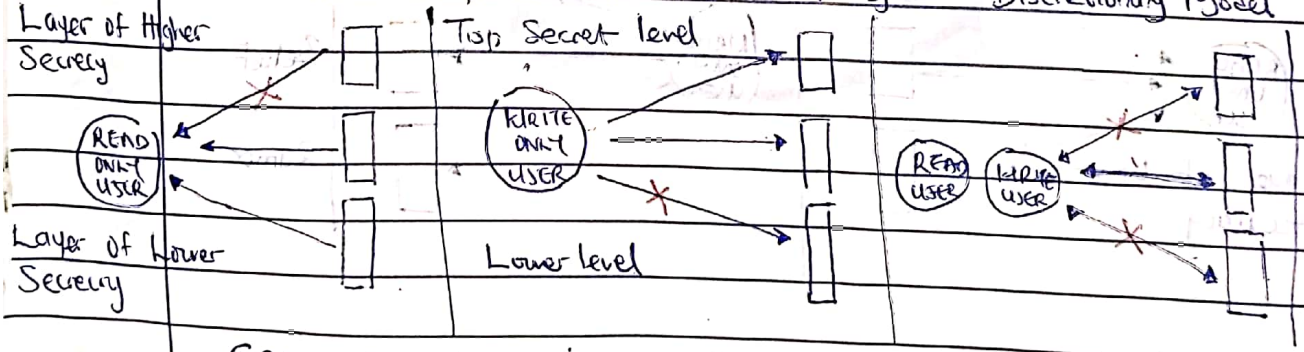
The Bell Lapadulla Model is a confidentiality model that is concerned with keeping sensitive data secure. It describes the MAC rules. In this model Security/Sentivity labels are used for Subjects while clearances are used for objects. With this model, all objects must be labeled from the most sentive (Top Secret) down to the least sensitive (public). Systems are divided into users (Subjects) and labeled objects - All objects must have a label for the system to work properly. This is considered a state machine with a set of allowable system states. Thus preserving the security of information even as the system moves from one state to another using the information flow model

Some properties are used with this model:

① The Star property → (No write Down) NWD - It prevents subjects with high level data clearance from writing the information to objects of lower access (no copy or paste into lower level) Thus preventing leakage. → No dividing of Secrets

② SIMPLE SECURITY PROPERTY → (No read Up) NRU - It prohibits reading up for confidentiality → No stealing of Secrets

③ Uses an access matrix of subjects and labeled objects to determine which subjects are permitted to access which objects - Discretionary Model



GRAPHICAL REPRESENTATION OF BELL-LAPADULA MODEL

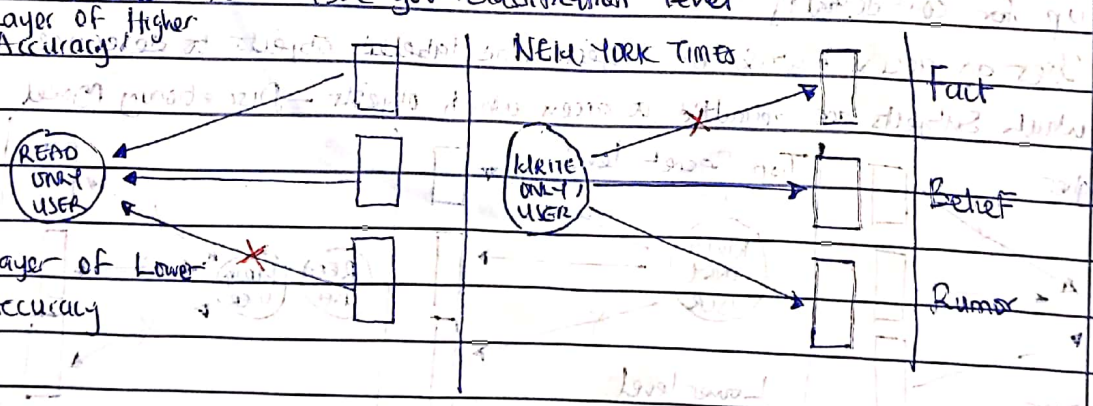
They are not permitted to read from a higher layer of secrecy but they can read from their layer and even from a lower layer of secrecy.	User is permitted to write data to the Top Secret and Secret level, but cannot write to the lower level as it could allow sensitive data to be released to individuals without Clearance	This user is permitted to read and write at their level only, but dont have access to read/write at higher or lower levels
SIMPLE SECURITY PROPERTY	*(STAR) PROPERTY	STRONG STAR PROPERTY
Simple is Reading e.g Loading from a disk	Star is writing Saving to a disk	Only Same level

BIBA MODEL → BIBA SYSTEM INTERGRITY MODEL

It is concerned with data integrity to make sure that data is not modified without authorization. In this model, integrity levels are used which are called Sensitivity levels in Bell-Lapadula. These rules will prohibit users from making inappropriate modification of data and prevent the corruption of data caused by introducing unreliable informations. Here an authentication process prevents unauthorized users from making modifications. MAC is used as well as the lattice model. Some properties used with this model include:

① No Write Up (NWU) and No Read Down (NRD) → Meaning Subjects cannot read objects of lesser integrity (trust level) and Subjects are not permitted to write data from a layer of lower integrity of trust to a higher level of trust → Prohibited from WURD

② Invocation Property → Means users cant request any services from an object with a higher integrity level. This means if you have a Secret classification you are not allowed to request anything from a Top Secret user because that's above your classification level



Readers are permitted to read from their level as well as a higher level of accuracy but cannot access any info at the lower level of accuracy

Writers are permitted to write to their level or below but cant write any data to the higher level

Scanned with CamScanner

Do not write in this Margin

UNIVERSITY OF BENIN

Question.....

Write on both side of the paper

39683

Do not write in this Margin

CLARK & WILSON INTERGRITY MODEL

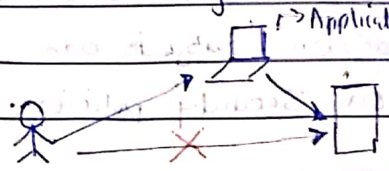
It is an integrity model like the Biba model It is an integrity verification procedure for constrained items. Applications are used to control the users (Subject) interaction with objects or programs. This model addresses 3 integrity goals:

① User Authentication and authorization with Access Control Lists to prevent unauthorized users from making modifications on the Systems

② It attempts to prevent any authorized or unauthorized users or processes from making improper modifications, by putting controls in place

③ Maintains consistency for both internal and external transactions. by using well formed transactions...

This model requires well formed transactions and requires that steps be performed exactly as listed in a defined order. Also the individuals performing the steps must be authenticated in order to be able to know who was responsible for making changes. The Clk models calls for a separation of Duties between IFE Administrators & the Users. Such that Users should not have administrative capabilities It also has a Take-Grant Model which helps administrators to pass on rights. They grant authenticated Users rights and privileges and leave it up to the subject whether to give rights to another, take or revoke rights.



The User is permitted to interact with ~~the Object only through the authorized~~ mechanism of going through the application. They are not permitted to interact with the object directly.

KEY TERMS

* SUBJECT → A user that is attempting to access some type of object or resource. Subjects can have different access levels, for example an administrator, A standard user. An example of a subject would be a User, process or a machine, infact anything attempting to access an object

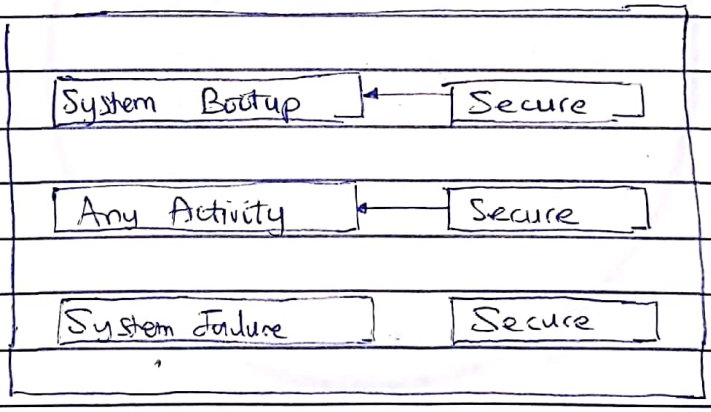
* OBJECT – It is a resource. They are passive entities that contain information that a user wants to access. An example is a file, a record in a database, a memory location

* ACCESS – The flow of information between the Subject and the Object. It is basically the ability of the subject to perform a task or an interaction with an object. It is very important to control access between Subject and Object to make sure that unauthorized individuals do not access resources that they should not be accessing

There are some commin security models that we can use to make sure that the interactions between our Subjects and Objects are acceptable and are based on our Security policies. They include ① State Machine Model

STATE MACHINE MODEL

It is an abstract model used by all computer systems, it does not specify protection mechanisms or means of enforcing the model. It deals with various states of operation or system states and has a set of values for each of these initial states, so depending on the state the system is operating in, there is a sequence of events that must be performed before the system can transform into the next stage. And the output and the next stage depends on the input and the present stage, what we mean is no matter what the system is trying to do, such as booting up, system failure, this model is concerned with making sure that the system is secure at each state and making sure that the intended sequence of events is followed.



The SMM works with security levels, classification and clearances
The SMM are majorly of two types/MODE

① SINGLE-STATE MACHINE MODEL - There is a policy in place that dictates the security levels of that system. The system will only process data from a single security level, hence the name. There are no separate classifications on the system because all of the data is at the same security level and all users have to have formal approval and full clearance to access all of the data on the system

(2) MULTI-STATE MACHINES MODEL

Here data can be processed at two or more security levels without the risks of compromising the System Security. The data can classified or unclassified and not all users require full clearance. This type is less secure compares to the Single State-Machine but they are more flexible. For example, you can have a System that processes Secret Data as well as Unclassified Data, Only the users with the Secret clearance will be able to access Secret data but any user will be able to access the unclassified data.

LATTICE BASED SECURITY MODEL

This model use a two dimensional matrix to define which subjects are permitted/allowed to access which objects at what permission level. It uses pairs of elements (which are subjects and objects) and each of these pairs has an ordered set with a lower band and an upper bound that defines their access rights. Most times those bounds (or limits) are set up using confidentiality levels (classifications and clearance levels like Bell lapadula) or integrity levels (like Biba). It finds its application in complex environments and allows to place security controls that will work for those environments.

Confidential	Upper Boundary	
Private	↑	Lattice of Permission Available for User
Sensitive	↕	
Public	↓ Lower Boundary	

Here the User is limited from accessing any confidential information because of their upper boundary and are also limited from doing anything at the public level because of their lower boundary They are only permitted to operate at the Private and Sensitive levels

NON INTERFERENCE MODEL

The idea is to prevent individuals from interferring with other individuals. So preventative controls are effected. It is done by putting users in separate areas called domains. A Domain is a set of objects that a user can access. The user at one level will not be able to tell what is happening at a higher Security level while those at the higher Security level would not be able to interfere with individuals at levels below them - This model uses a state machine approach to keep track of which actions are allowed for which user. It makes sure that users in one domain do not affect or interfere with users in another domain and users cannot be influenced by actions/behaviors of other subjects at higher Security levels