Classic Information Security Models

19CSE311 Computer Security

Jevitha KP

Department of CSE

Security Models

- Security models are used to **determine how security will be implemented**, what subjects can access the system, and what objects they will have access to.

- They are a way to formalize security policy.

- These models are used for maintaining goals of security, i.e. **Confidentiality, Integrity, and Availability** - deals with **CIA Triad maintenance.**

- These models lays out broad guidelines and is not specific in nature

- No organization can secure their sensitive information or data without having effective and efficient security models.

- They are the key components that have to be taken into consideration when engineering security systems and policies.

Security Policy vs Security Models

- **Security policy** is a document that expresses clearly and concisely what the **protection mechanisms** are to achieve. Its a statement of the security we expect the system to enforce.

- A security model is a scheme for specifying and enforcing **security policies**:

  - it describes the entities governed by the policy,

  - it states the rules that constitute the policy.

Types of Security Models

- There are various types of security models:
  - Models can **capture policies for confidentiality** (Bell-LaPadula) or for **integrity** (Biba, Clark-Wilson).
  - Some models **apply to environments with static policies** (Bell-LaPadula),
  - Some consider **dynamic changes of access rights** (Chinese Wall).
  - Security models can be
    - informal (Clark-Wilson),
    - semi-formal, or
    - formal (Bell-LaPadula, Harrison-Ruzzo-Ullman).

Classic Security Models

- **Bell-LaPadula Model**
- **Biba Model**
- **Clark Wilson Model**
- Brewer and Nash Model (Chinese Wall Model)
- Harrison-Ruzzo-Ullman Model

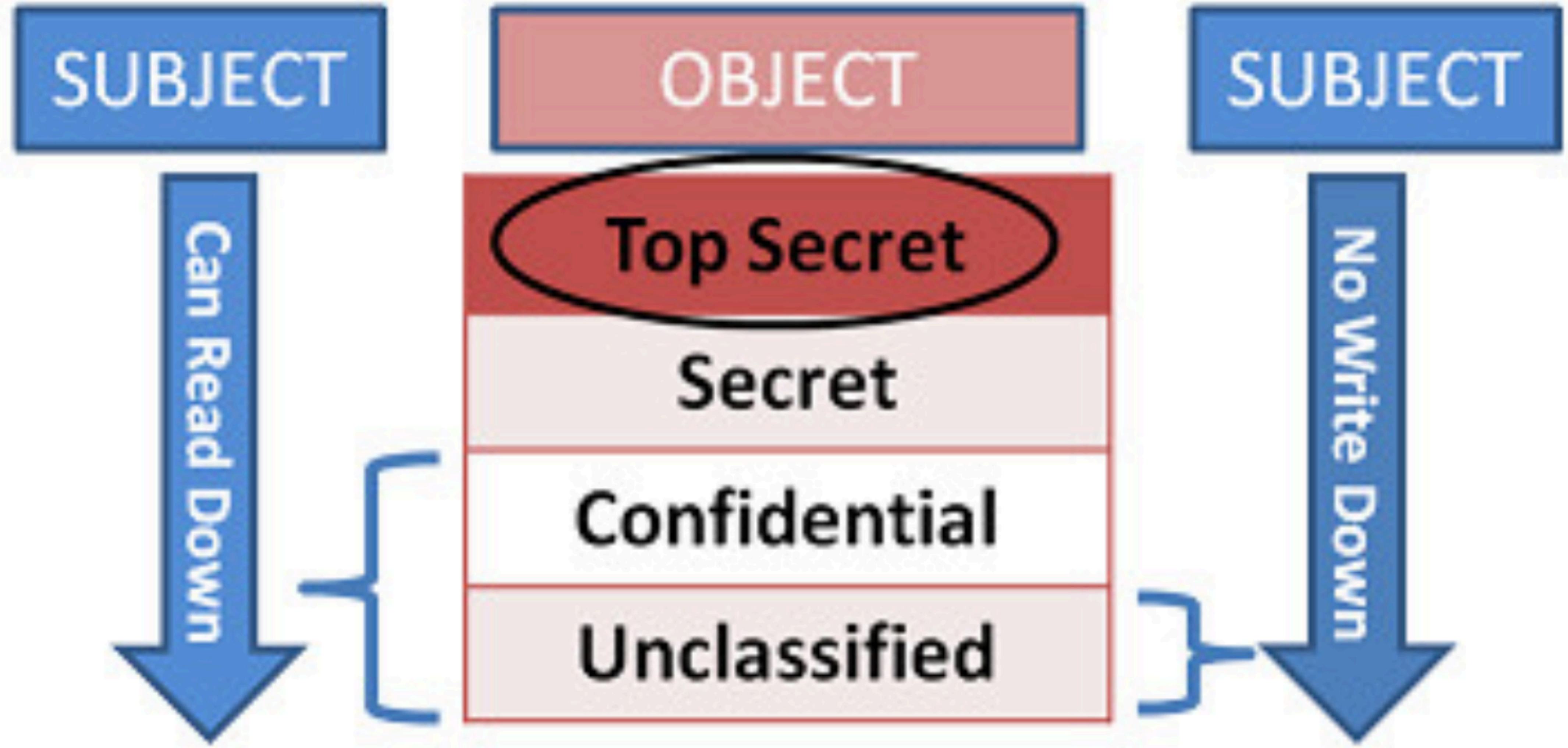
Bell-LaPadula Model

- The model of Bell-LaPadula was originally done the development of the US Department of Defense (DoD).

- It was invented by Scientists David Elliot Bell and Leonard .J. LaPadula and hence called **Bell-LaPadula Model**.

- This is used to maintain **Confidentiality** of CIA.

- Here, the classification of **Subjects(Users)** and **Objects(Files)** are organized in a **non-discretionary** fashion, with respect to different layers of secrecy.


SUBJECT
OBJECT
SUBJECT
Can Read Down
Top Secret
Secret
Confidential
Unclassified
No Write Down

Bell-LaPadula Model

- It has mainly 3 Rules:
- **SIMPLE CONFIDENTIALITY RULE:**
  - Simple Confidentiality Rule states that the **Subject** can only **Read the files on the**
    - **Same Layer of Secrecy** and the **Lower Layer of Secrecy**
    - **but not the Upper Layer of Secrecy**, due to which we call this rule as **NO READ-UP**

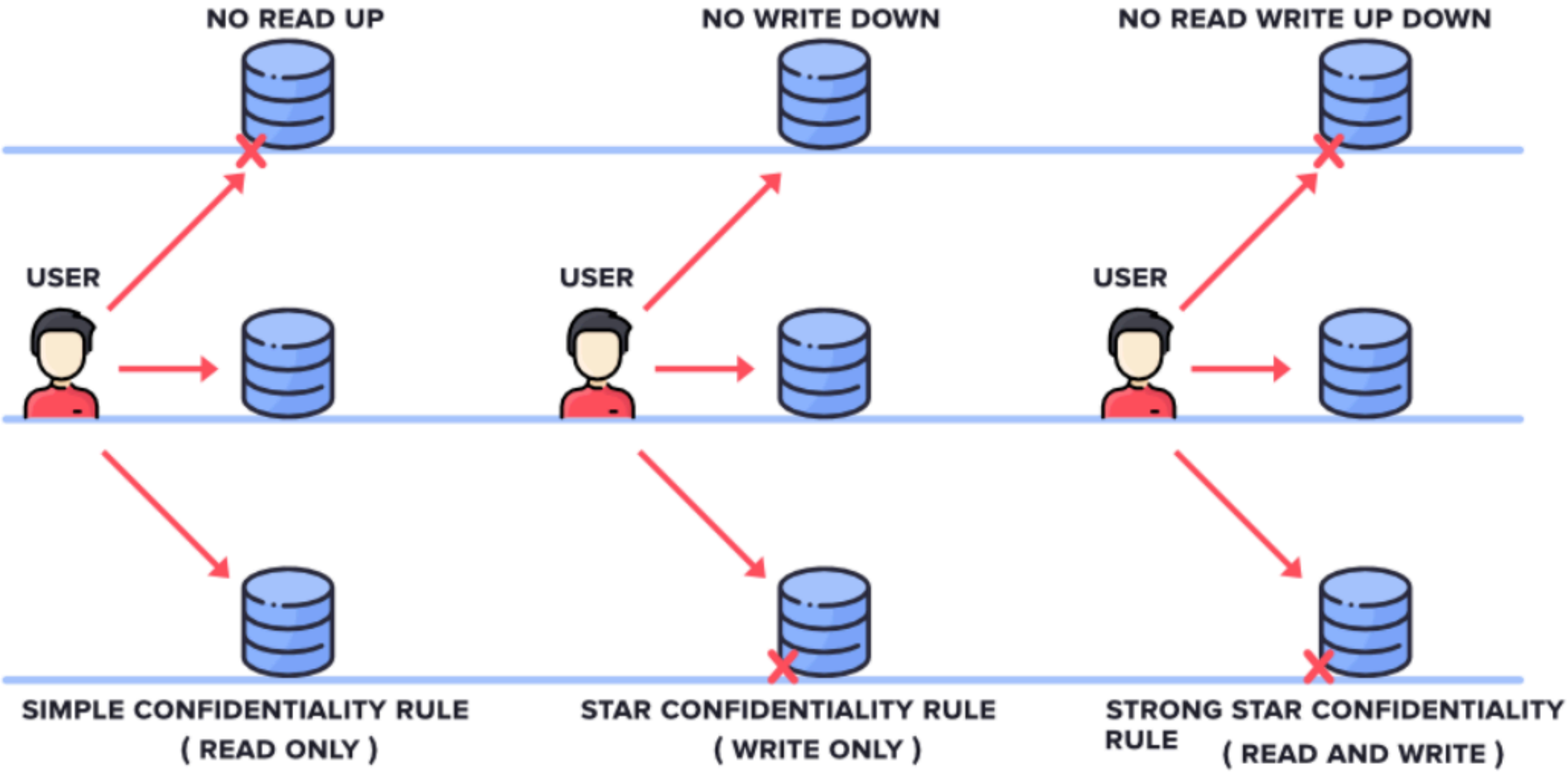
Bell-LaPadula Model

- **STAR CONFIDENTIALITY RULE:**
    - Star Confidentiality Rule states that the **Subject** can only **Write the files on the**
        - **Same Layer of Secrecy and the Upper Layer of Secrecy**
        - **but not the Lower Layer of Secrecy**, due to which we call this rule as NO WRITE-DOWN

Bell-LaPadula Model

- **STRONG STAR CONFIDENTIALITY RULE:**
  - Strong Star Confidentiality Rule is **highly secured** and **strongest** which states that the **Subject can Read and Write the files** on the
    - Same Layer of Secrecy only and
    - not the **Upper Layer of Secrecy or the Lower Layer of Secrecy**,
    - due to which we call this rule as **NO READ WRITE UP DOWN**

BELL - LAPADULA MODEL



NO READ UP

NO WRITE DOWN

NO READ WRITE UP DOWN

USER

USER

USER

SIMPLE CONFIDENTIALITY RULE
(READ ONLY)

STAR CONFIDENTIALITY RULE
(WRITE ONLY)

STRONG STAR CONFIDENTIALITY RULE
(READ AND WRITE)

Bell-LaPadula Model

- **Tranquility principle:**
  - The tranquility principle of the Bell–LaPadula model states that the **classification of a subject or object does not change** while it is being referenced.
  - There are two forms to the tranquility principle:
  - **Principle of Strong Tranquility** states that security levels do not change during the normal operation of the system.
  - **Principle of Weak Tranquility** states that security levels may never change in such a way as to violate a defined security policy.
    - Weak tranquility is **desirable** as it allows systems to observe the **principle of least privilege.**
    - Processes start with a low clearance level regardless of their owners clearance, and **progressively accumulate higher clearance levels** as actions require it.

Bell-LaPadula Model

- Advantages:
  - a **subject may not downgrade information**
  - objects and subjects cannot change security levels once instantiated.

Bell-LaPadula Model

- **Disadvantages**:
  - Users can never talk to ”low” users.
  - Model only addresses confidentiality but does not addresses access control or covert channels.
  - Anyone can create a higher classification object.
  - Although the BLP model was initially created to fulfill Department Of Defense (DoD, US) requirements for information security, the military is currently achieving these goals through the use of **discretionary access control and segregation,** instead of the BLP model.

Biba Model

- This Model was invented by Scientist Kenneth .J. Biba. and hence the model is called Biba Model.

- This is used to maintain the **Integrity** of Security.

- Here, the classification of **Subjects(Users) and Objects(Files)** are organized in a non-discretionary fashion, with respect to different layers of secrecy.

- This works the exact reverse of the Bell-LaPadula Model.

Biba Model

- It has mainly 3 Rules:
- **SIMPLE INTEGRITY RULE:**
  - Simple Integrity Rule states that the **Subject** can only **Read the files** on the
    - Same Layer of Secrecy and the Upper Layer of Secrecy
    - but not the Lower Layer of Secrecy, due to which we call this rule as **NO READ DOWN**

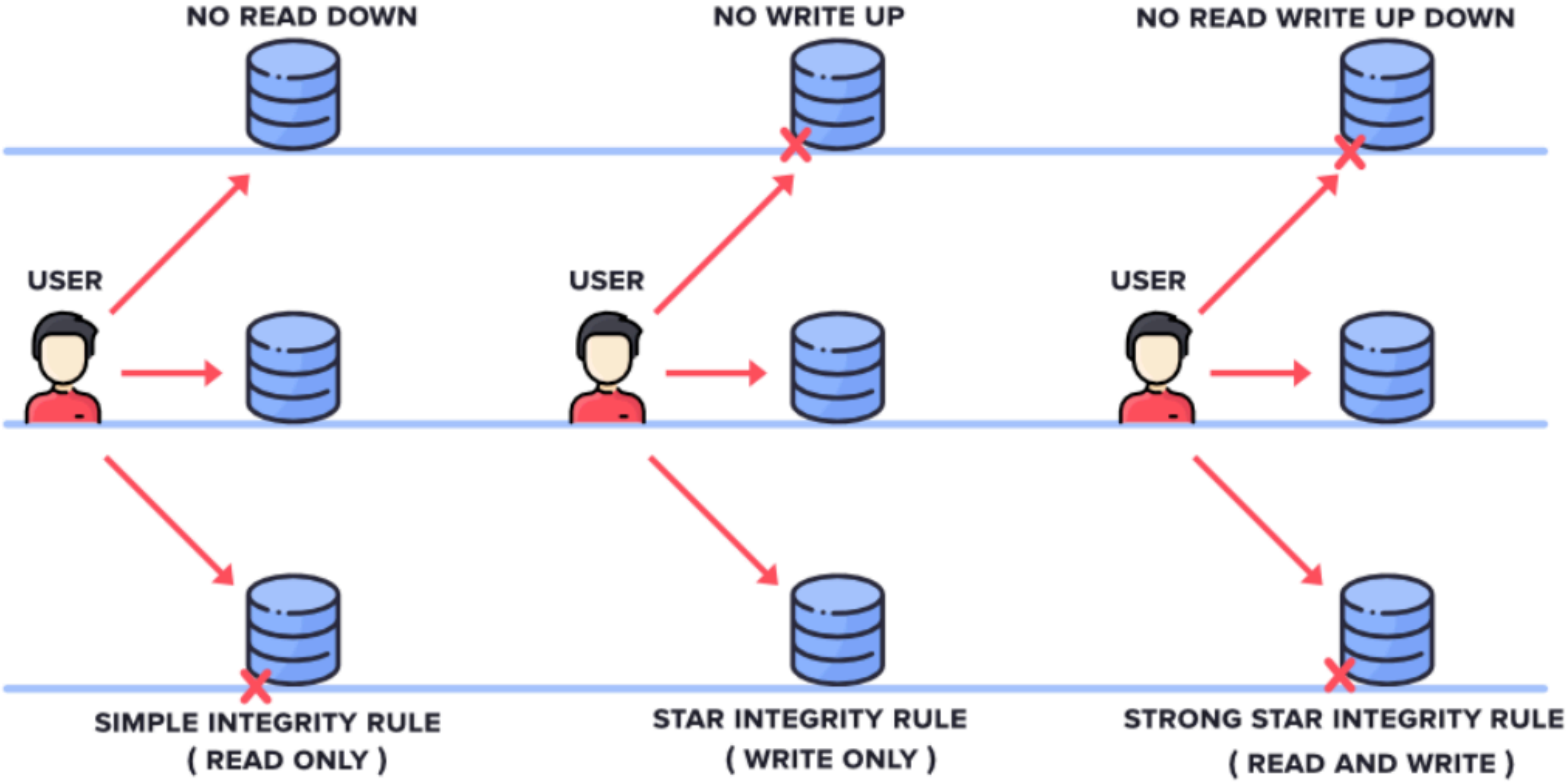
Biba Model

- **STAR INTEGRITY RULE:**
  - Star Integrity Rule states that the **Subject** can only **Write the files** on the
    - Same Layer of Secrecy and the Lower Layer of Secrecy
    - but not the Upper Layer of Secrecy, due to which we call this rule as **NO WRITE-UP**

Biba Model

- **STRONG STAR INTEGRITY RULE**
- Strong Star Integrity Rule states that the **Subject can Read and Write the files on the**
  - Same Layer of Secrecy only and
  - not the Upper Layer of Secrecy or the Lower Layer of Secrecy,
  - due to which we call this rule as **NO READ WRITE UP DOWN**

BIBA MODEL



NO READ DOWN

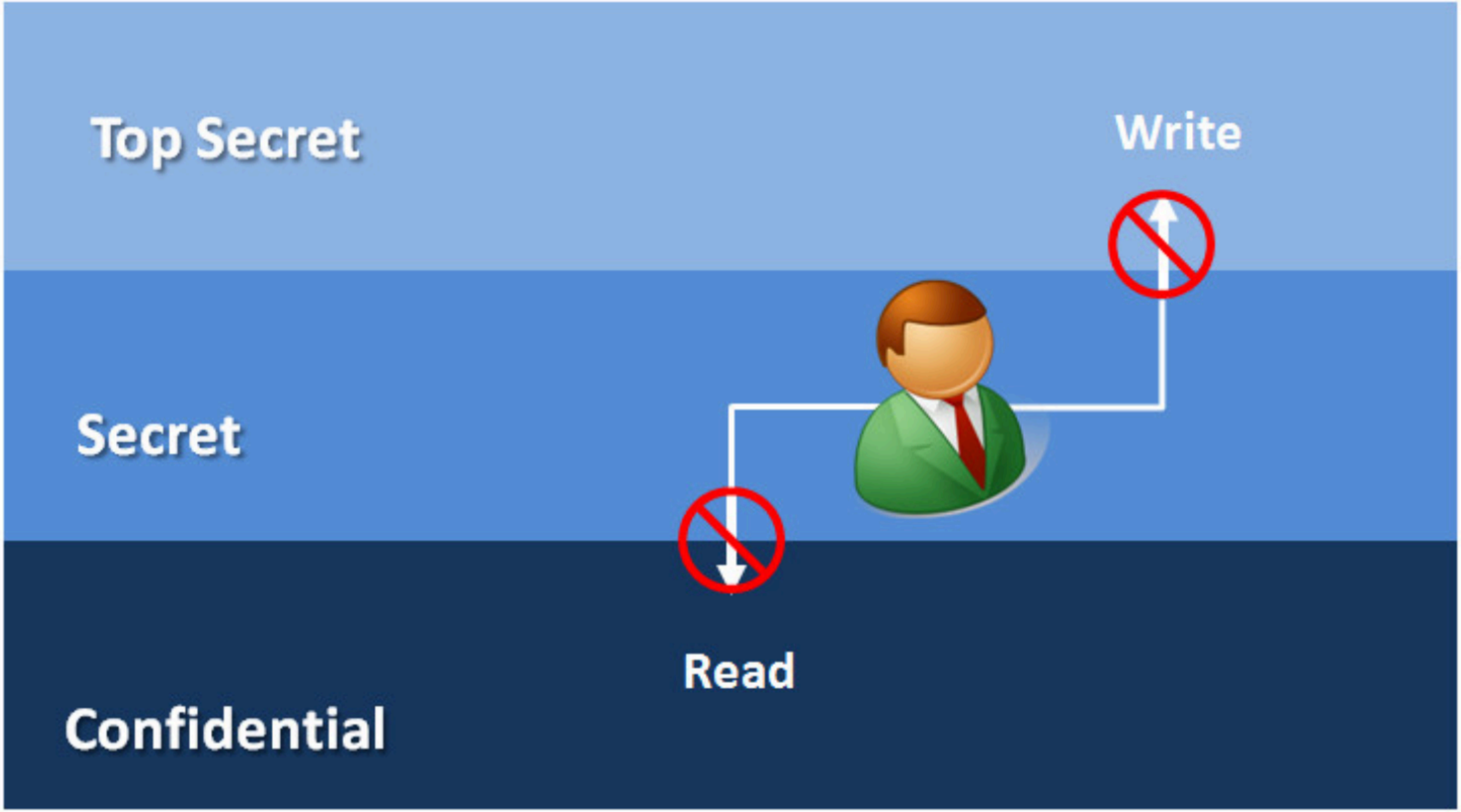
NO WRITE UP

NO READ WRITE UP DOWN

SIMPLE INTEGRITY RULE
(READ ONLY)

STAR INTEGRITY RULE
(WRITE ONLY)

STRONG STAR INTEGRITY RULE
(READ AND WRITE)



Top Secret

Write

Secret

Read

Confidential

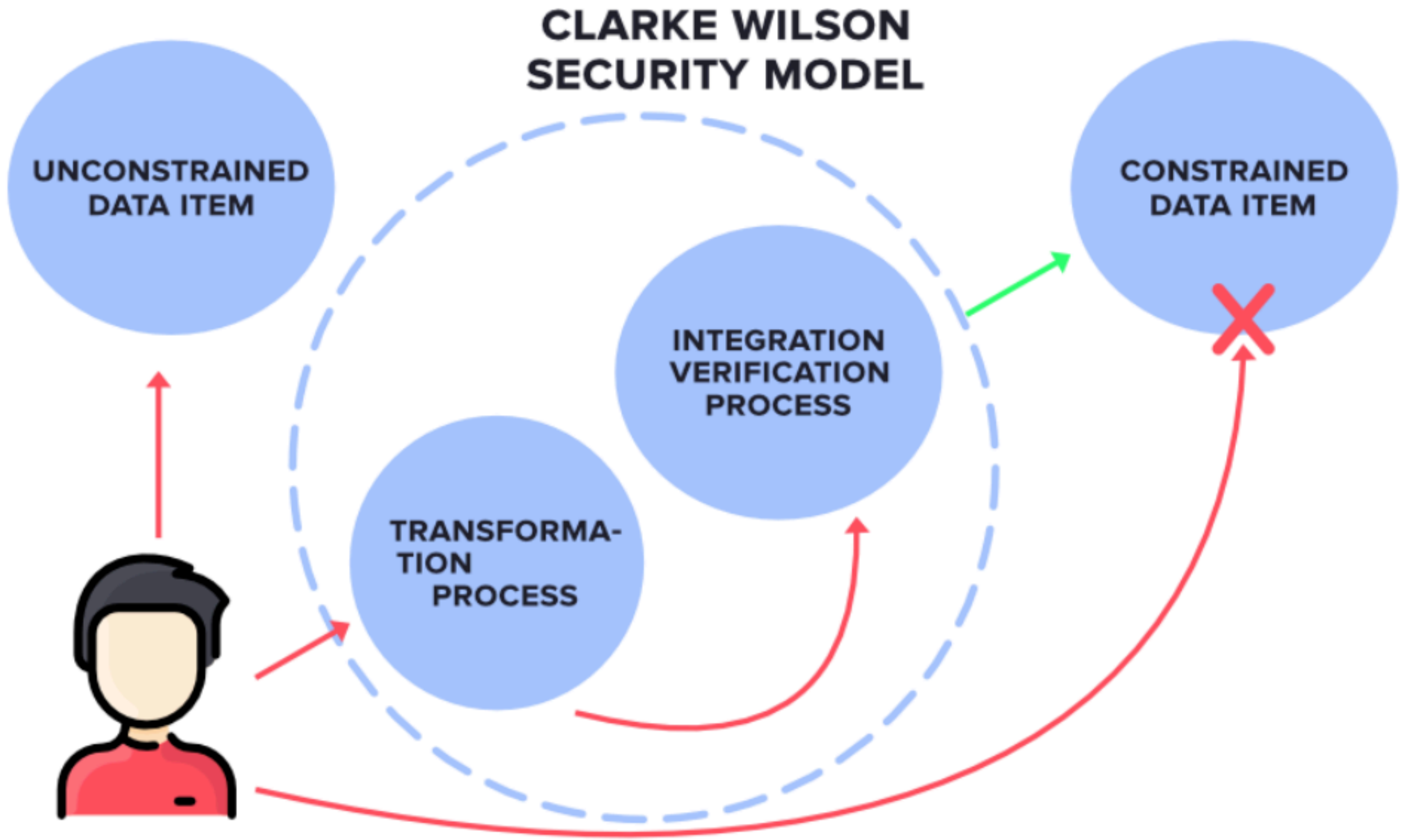
Biba Model

- There is no “read-down” because **lower integrity cannot be read by high integrity.**

- And there is no “write-up” because **subjects cannot move low integrity data to high integrity environments.**

Clarke Wilson Security Model

- This Model is a highly secured model. It has the following entities.
  - **SUBJECT**: It is any user who is requesting for Data Items.
  - **CONSTRAINED DATA ITEMS (CDI)**: It cannot be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model
  - **UNCONSTRAINED DATA ITEMS (UDI)**: It can be accessed directly by the Subject.



CLARKE WILSON SECURITY MODEL

UNCONSTRAINED DATA ITEM

INTEGRATION VERIFICATION PROCESS

TRANSFORMATION PROCESS

CONSTRAINED DATA ITEM

Clarke Wilson Security Model

- **TRANSFORMATION PROCESS (TP)**:
  - Here, the **Subject's request** to access the **Constrained Data Items** is handled by the **Transformation process**
  - **Transformation process** converts it into **permissions** and then forwards it to **Integration Verification Process**
- **INTEGRATION VERIFICATION PROCESS (IVP)**:
  - The Integration Verification Process will perform **Authentication and Authorization.**
  - If that is successful, then the Subject is given access to **Constrained Data Items.**

Brewer—Nash (Chinese Wall)

- This model provides access controls that can **change dynamically** depending upon a user's previous actions.

- The main goal of this model is to **protect against conflicts of interests** by user's access attempts.

- It is based on the **information flow model,** where no information can flow between subjects and objects in a way that would result in a **conflict of interest.**

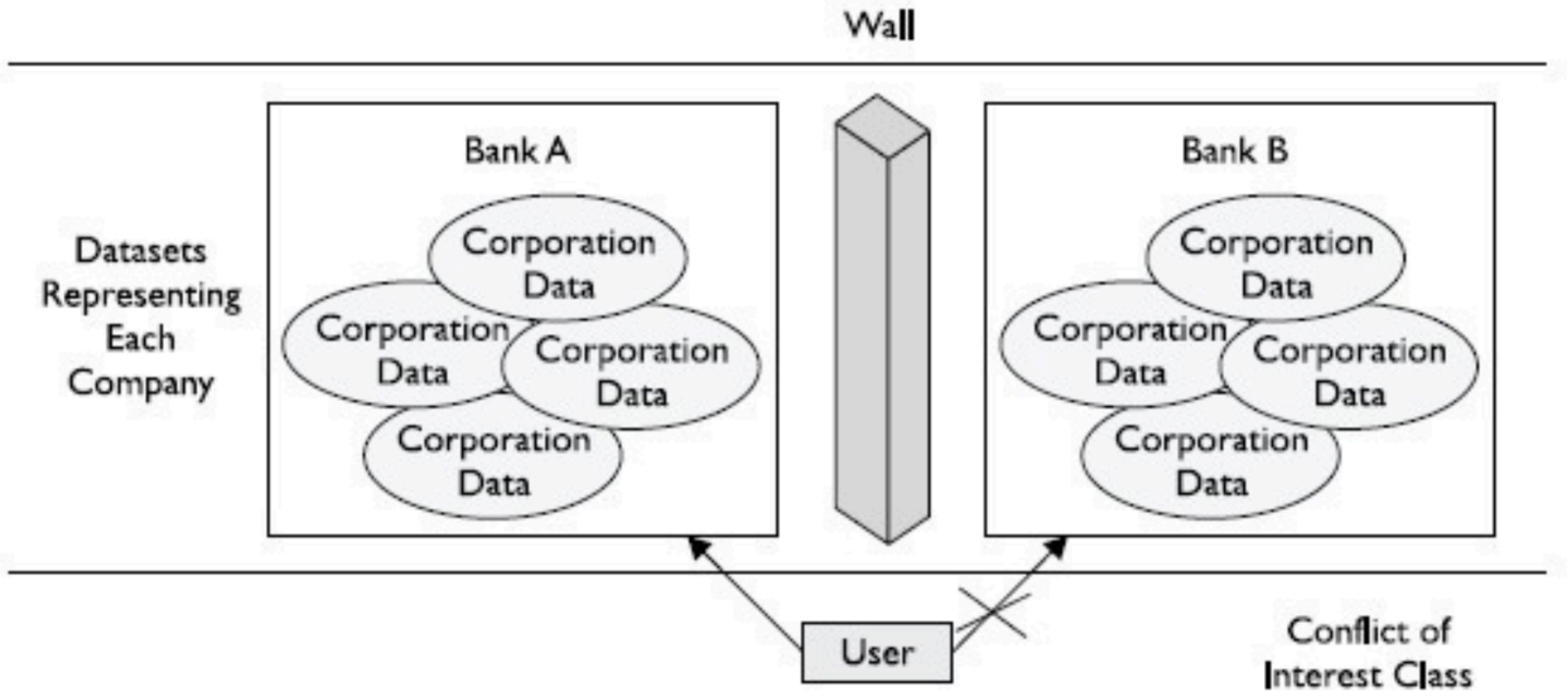
- The model states that a subject can write to an object if, and only if, the subject can not read another object that is in a different data set.

Brewer—Nash (Chinese Wall)

- The Chinese Wall model's principle is focused on conflict of interest where a **certain user should not be accessing confidential information** belonging to **two separate interested and/or participating stakeholders.**

- Access control policies change based on user behavior.

- In other words, once you access the data belonging to one side, the other side's data becomes unavailable or inaccessible.



Wall

Datasets Representing Each Company

Bank A

Corporation Data

Corporation Data

Corporation Data

Corporation Data

Bank B

Corporation Data

Corporation Data

Corporation Data

Corporation Data

User

Conflict of Interest Class

Harrison—Ruzzo—Ullman Model

- The HRU security model (Harrison, Ruzzo, Ullman model) is an operating system level computer security model which deals with the **integrity of access rights** in the system.

- The system is based around the idea of a **finite set of procedures** being available to edit the access rights of a subject s on an object o.

- The model also discussed the possibilities and limitations of **proving safety of a system** using an algorithm.

Harrison—Ruzzo—Ullman Model

- The Harrison–Ruzzo–Ullman model could be considered an add-on to the BLP model.
- The BLP model has no mechanisms for changing access rights or for the creation and deletion of subjects and objects.
- The HRU model addresses these issues by defining an **authorization system** to allocate access rights and verifying compliance with any given policy preventing non-authorized access.
- The HRU model can be implemented via an **Access Control List or via a Capabilities list.**

Which model to choose?

- In today’s communication environments the best options to implement out of the five models discussed are
  - the Clark-Wilson model and
  - the Harrison-Ruzzo-Ullman model.
- HRU deals with multilevel security at the OS level and the CW model can be applicable to a wide range of industry applicability.
- The other models are not up to standards for today’s security threats.
- BLP only covers static relationships, which is not realistic, and the Chinese Wall is not useful in the real world, apart from a legal environment application.
- Implementation of the Biba model is also not practical since it does not take into account malicious intentions from the user.

Last two models are not for exams

Additional Reading

- https://media.techtarget.com/searchSecurity/downloads/29667C05.pdf
- https://www.linkedin.com/pulse/security-models-integrity-confidentiality-protection-data-justiniano
- https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models