Chapter-#04

Cyber Security **Models**

Cyber Security **Models**

- The security models are specifically defining the relationship of operating system performance with the information security models. The effective and efficient security models secure the sensitive and relevant information or data of the organizations. The security policy is verified by using the information security models. They deliver a precise set of directions to the computer to follow the implementation of vital security processes, procedures, and concepts contained in a security program. They define the security concern in information threads.

- Security models are used to evaluate and authenticate the security policy to map the intellectual property of the information system. They are used to represent the mathematical and analytical ideas that are developed by programmers. These ideas are mapped with the system specifications through programming code.

Cyber Security **Models**

- These ideas maintain the goal of CIA property that is confidentiality, integrity, and availability. The CIA properties are elaborated in detail.
- **Confidentiality**
- Confidentiality refers to protecting the data from unauthorized access. Only legitimate users can access sensitive information. The main goal of confidentiality is to stop information from getting into the wrong hands. There are many ways to secure data confidentiality such as use of strong passwords, authentication, data encryption, segregation of data and so forth. Some common threats that exist are against the rules of confidentiality.
- Encryption cracking.
- Eavesdropping attack.
- Malicious insiders.
- Man-in-the-middle attack.

Cyber Security **Models**

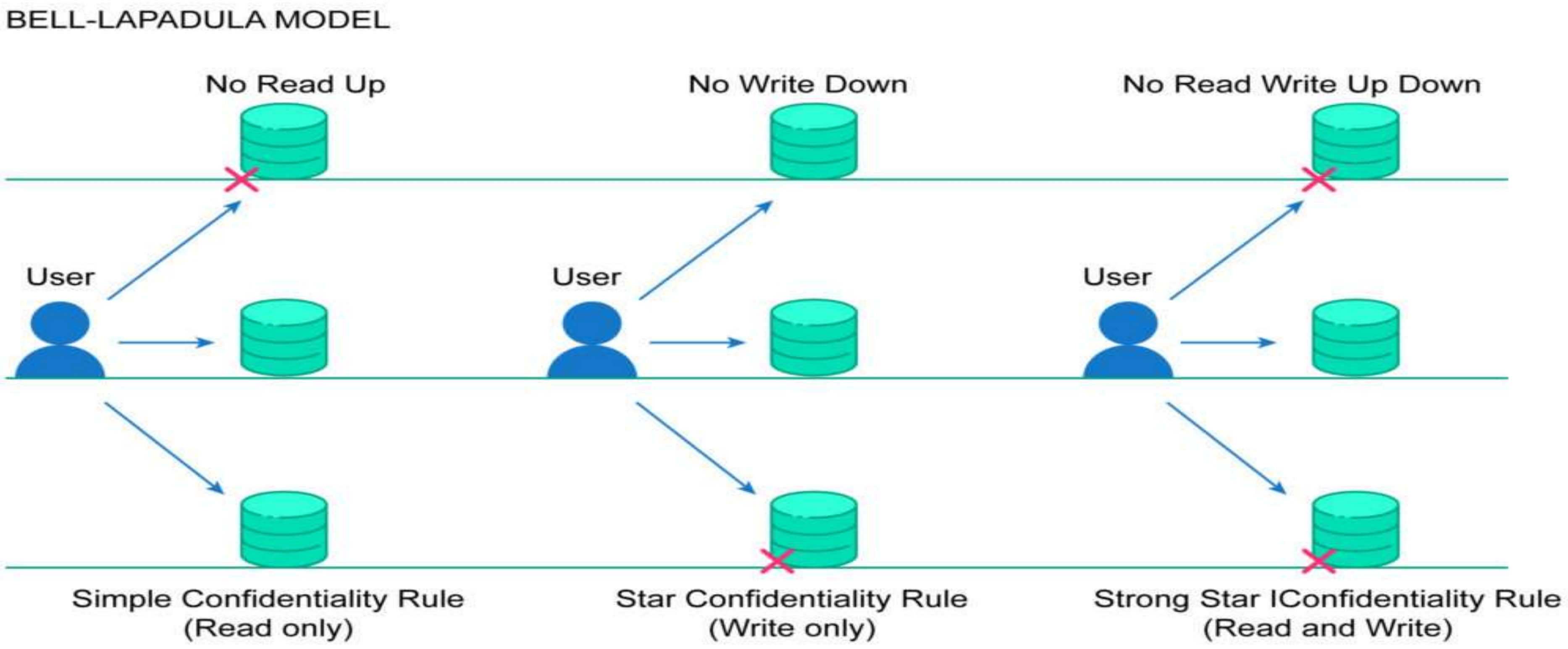
- **Integrity**
- Integrity is used to validate the information. It checks whether the information present is in correct format or not. It also validates information that is true and correct to its original purposes. Integrity ensures that the receiver's information is the same as the creator's information. The information can be edited only by the legal person to prevent unwanted modification. There are no rights provided to anyone to change or modify the data. In some cases, electromagnetic pulse (EMP) or server crashes are responsible to break the integrity.
- So, integrity ensures the accuracy, trust worthiness, and validity of data throughout its life cycle. It holds value if it is truthful. There must be mechanisms to restore data in case of unintended changes. Some challenges that could affect the integrity of information are
- Physical compromise to device.
- Human error.
- Data encryption and hashing are the mechanisms that are used to preserve integrity.

Cyber Security **Models**

- **2 Availability**
- This implies that the network should be accessible to its users at all times. This holds true for both systems and data. To ensure network availability, network administrators should maintain hardware, perform regular upgrades, have a fail-over plan, and avoid bottlenecks. Attacks such as DoS or DDoS can make a network unusable as the network's resources are depleted. Companies and users who rely on the network as a business tool may suffer from a substantial impact. As a result, sufficient precautions should be taken to avoid such attacks.
- Threat to information availability occurs due to many reasons such as:
- Malicious Code.
- Insufficient bandwidth.
- DDOS (Distributed Denial of Service attack).
- **There are three main types of classic security models** namely
- Bell-LaPadula model
- Biba model
- Clarke Wilson Security model

Cyber Security **Models**

- **Bell-LaPadula model**
- This model was invented by **David Elliot Bell** and **Leonard.J. LaPadula** and therefore, this model is known as **Bell-LaPadula**. This model is used to ensure the confidentiality of information. It defines the functions of a multilevel security system. It is the first mathematical model that prevents secret information from being accessed in an unauthorized manner. In this picture, the user and the files are arranged in a non-discretionary manner concerning different layers of secrecy.

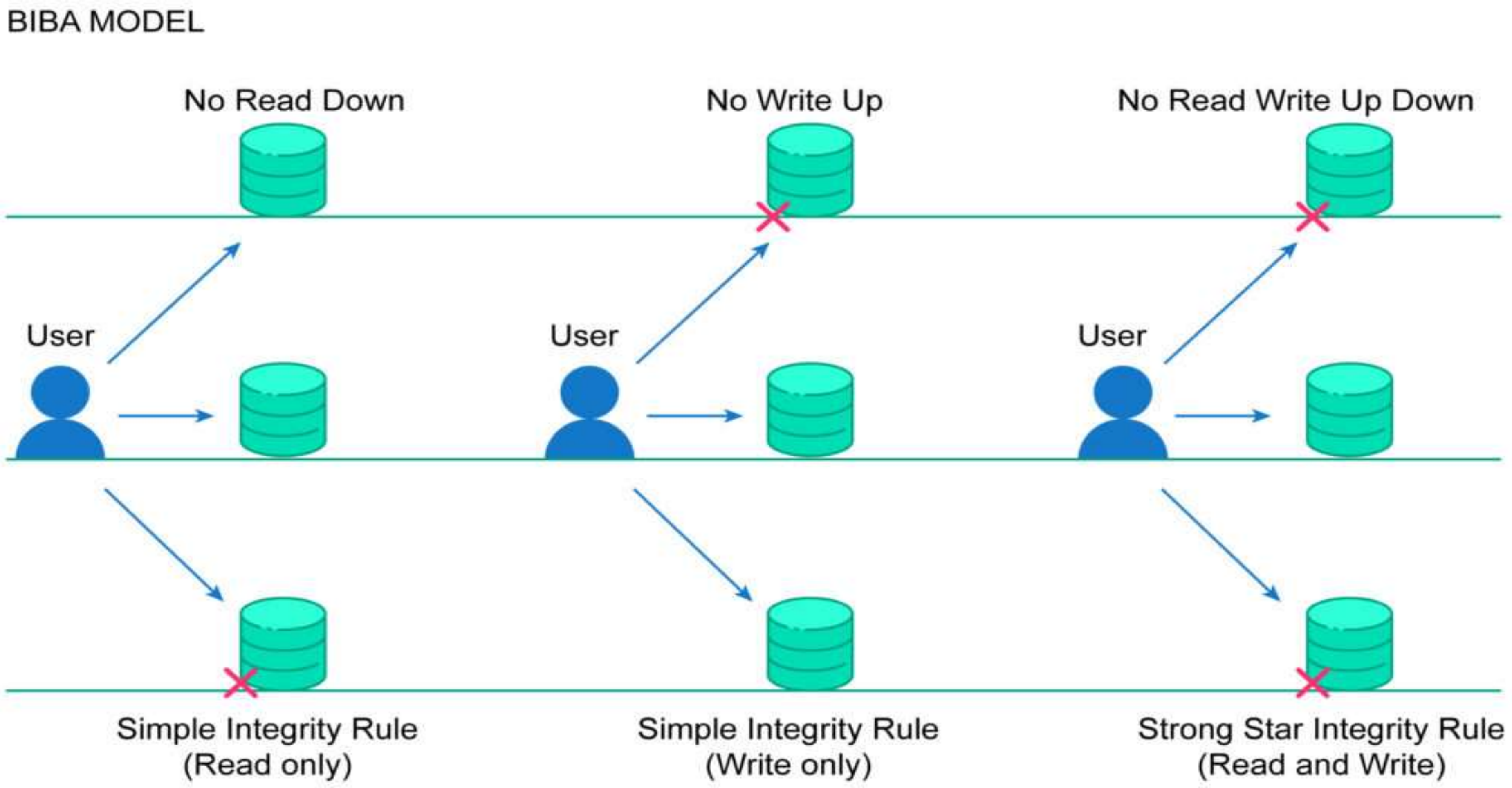


Cyber Security **Models**

- It follows three types of basic rules-
- Simple confidentiality rule
- Star confidentiality rule
- Strong star confidentiality rule
- **Simple confidentiality rule**
- This rule is called the NO READ-UP rule because it states that only the user can read the files that are on the same layer and lower layer of secrecy but cannot read the files on the upper layer of secrecy.
- **Star confidentiality rule**
- This rule is called the NO WRITE-DOWN rule because it states that the user can write the files on the same layer of secrecy and upper layer of secrecy but cannot read the files on the lower layer of secrecy.
- **Strong star confidentiality rule**
- This rule is called NO READ WRITE UP DOWN because the user can only read and write the files on the same layer of secrecy but cannot read and write the files on the upper layer of secrecy and the lower layer of secrecy. This is the highly secured and strongest rule in Bell-LaPadula.

Cyber Security **Models**

- **Biba model**
- The Biba model was named so after its inventor Kenneth.J. Biba. This model is used to ensure the integrity of information.

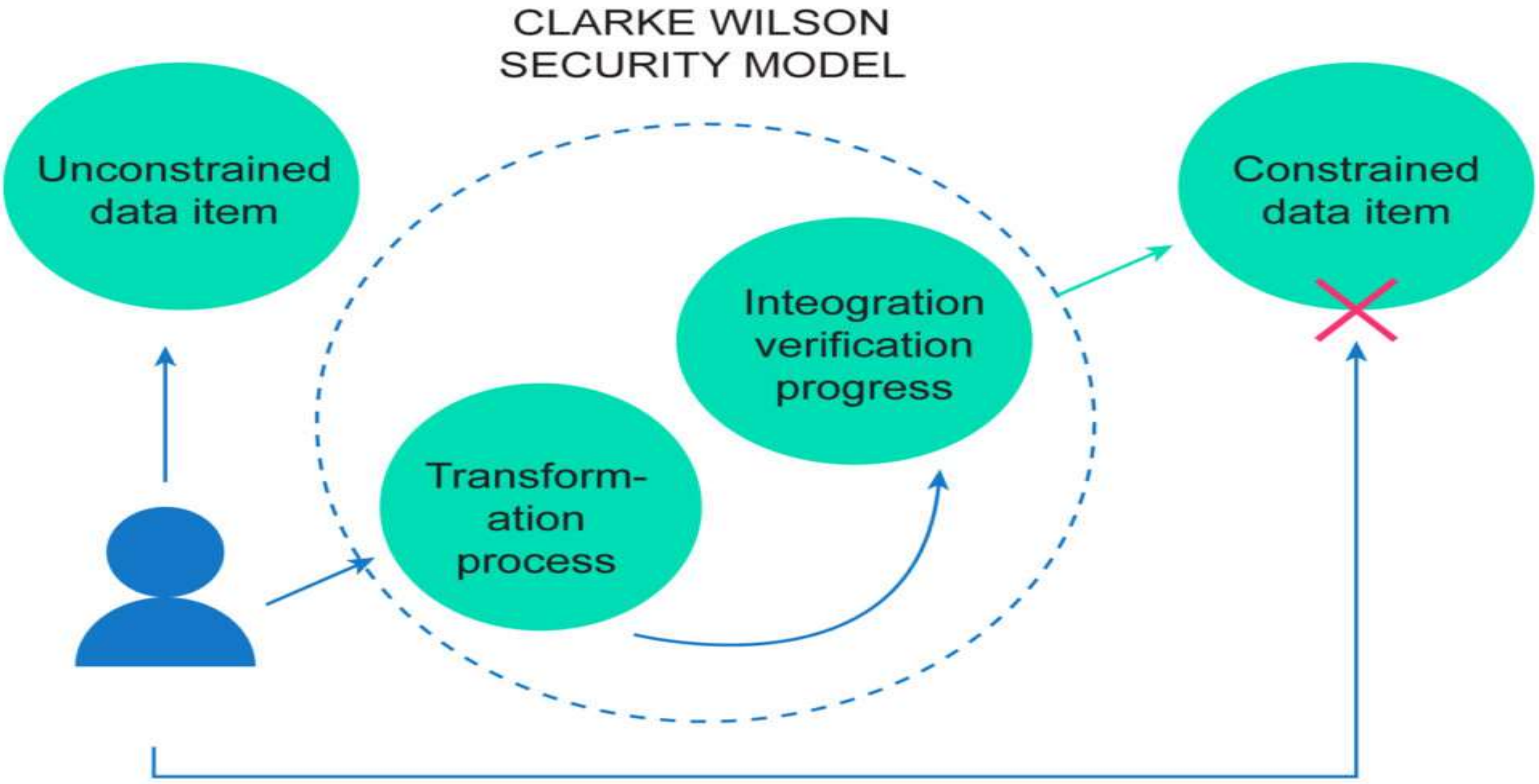


Cyber Security **Models**

- **It follows 3 rules:**
- Simple integrity rules
- Star integrity rules
- Strong star integrity rule
- **Simple integrity rules**
- This rule is called the NO READ-DOWN rule because the user can read the files only on the same layer of secrecy and upper layer of secrecy but cannot read the files on the lower layer of secrecy.
- **Star integrity rule**
- This rule is called the NO WRITE-UP rule because users can read the files only on the same and lower layer of secrecy but cannot read the files on the upper layer of secrecy.
- **Strong star integrity rule**
- This rule is called the NO READ-WRITE UP DOWN rule because the user can read and write the files on the same layer of secrecy only but cannot read and write the files on the upper or lower layer of secrecy. This rule is highly secured and is the strongest rule in Bell-LaPaulda.

Cyber Security Models

- **Clarke Wilson Security Model**
- This model provides the highest security to the security model. It has the following entities:



Cyber Security **Models**

- **Subject**
- It is the user who requests the data items.
- **Constrained data items**
- Users cannot access constrained data items directly. It is accessed according to the Clarke Wilson Security Model.
- **Unconstrained data item**
- Users can access it directly.
- The constrained data can be accessed by following processes:
- **1. Transformation process**
- The user can request constrained data items that are handled by the transformation process. The process converts it into permission and then forwards it to the integration verification process.
- **2. Integration verification process**
- It performs authorization and authentication. If this verification is successful, then the user is given access to the constrained data items.
- **Common Mistakes** There is a mistake in understanding the terms confidentiality and integrity. In simple language, confidentiality defines that the information should not go to the wrong hands. Integrity shows data validity. This means that only an authorized and legal person can access the authorized content or information.