Software System Security

POOJA PREMNATH

Unit 5

Security Policies

The Nature of Security Policies - Types of Security Policies - The Role of Trust; Confidentiality policy: The Bell-LaPadula Model; Integrity policy: Clark-Wilson Integrity Model; Availability Policy, Denial of Service Models; Hybrid policy: Chinese Wall Model

* Security Policy: A security policy is a statement of what is, and what is not allowed

* Security mechanism: A security mechanism is a method, tool or procedure for enforcing a security policy.

eg. → Suppose a university's computer science laboratory has a policy that prohibits any student from copying any other student's HW.

→ A fails to use these mechanisms to protect her HW files and B copies them.

→ A breach of security has occurred, because B has violated the security policy. A's failure to protect her files does not authorize B to copy them.

* Secure, Precise or Broad Security Mechanism:

→ Let P be the set of all possible states.

→ Let Q be the set of secure states as specified by the security policy.

→ Let the security mechanism restrict the system to set of states R
e $R \in P$.

→ Then a security mechanism is:

secure : $R \subseteq Q$

Precise : $R = Q$

broad : If there are states r such that $r \in R$ and $r \notin Q$.

* Access Control Matrix

→ An access control matrix is a conceptual model used in computer security to represent and manage access control policies.

→ It provides a structured way to define and view the access permissions for various subjects and objects (files, directories or resources)

	Object 1	Object 2	Object 3
Subject 1	Read, write	Read	-
Subject 2	Read	-	Read, Execute
Subject 3	-	write	Execute

* Types of Access Control

A. Discretionary Access Control - If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a discretionary access control (DAC), also called an Identity-based access control (IBAC)

→ In DAC, users or owners of resources have discretion over who can access those resources and what actions they can perform on them

B. Mandatory Access Control - when a system mechanism controls access to an object and an individual user can alter that access, it is called mandatory access control, also called rule-based access controls

→ In MAC, access rights are determined by the system rather than the resource owner.

C. ORCON - In originator controlled access control, access is based on the creator of an object or the information it contains

D. Fine-grained Access Control - applies multiple constraints/conditions to allow/deny access to other assets.

→ has a higher level of specificity and precision than other access control methods.

* Protection State - The term protection state refers to the current security or access control configuration of a system / process within a system.

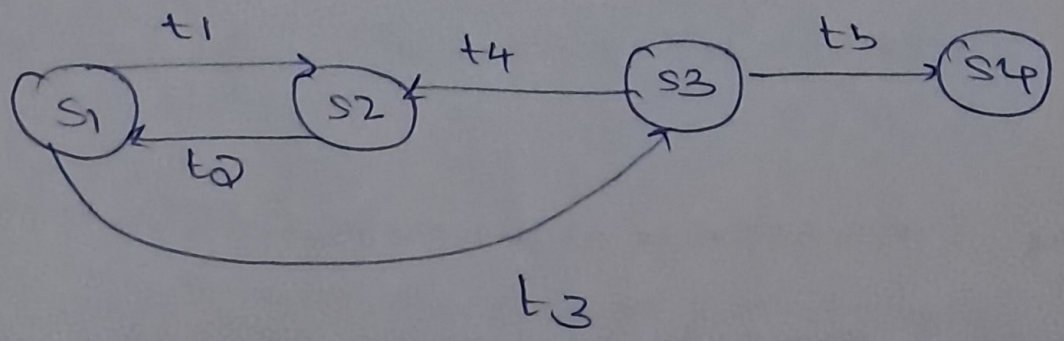
→ It reflects the level of protection afforded to resources and data within the system, as well as the permissions and restrictions placed on users / processes

* Security Policy Representation as an FSM

→ A security policy is a statement that partitions the states of the system into a set of authorized, or secure states and a set of unauthorized, or nonsecure states.

→ A secure system is a system that starts in an authorized state and cannot enter an unauthorized state.

→ A breach of security occurs when a system enters an unauthorized state.



The security policy for this FSM partitions it into

Authorized states = {S1, S2}

Unauthorized states = {S3, S4}

* CIA Triad for Security Policies

Confidentiality : Let X be a set of entities and let I be some information.

Then I has the property of confidentiality w.r.t X if no member of X can obtain information about I. (aims to find info leaks)

Integrity : Let X be a set of entities and let I be some info. or a resource. Then I has the property of integrity wrt to X if all members of X trust I. (defines authorized ways in which info may be altered)

Availability : Let X be a set of entities and let I be a resource. Then I has the property of availability wrt X if all members of X can access I. (describes which services must be provided)

* Policy Model

→ A policy model is a model that represents a particular policy or class of policies.

Types of Security Policies

A. Military Security Policy (also called a governmental security policy) is a security policy developed primarily to provide confidentiality

→ Unauthorized disclosure can result in penalties that includes jail or fines

B. Commercial Security Policy? → A security policy developed primarily to promote integrity?.

→ based on the notions of transactions. Like database specifications, they require that actions occur in such a way so as to leave the database in a consistent state.

→ These policies, called transaction-oriented integrity security policies, are critical to organizations that require consistency of databases

* Role of Trust in Security Policies

→ Confidentiality policies place no trust in objects, the object could be a factually correct report or a tale from Aesop's fables.

→ All that the confidentiality policy says is that the object should/ should not be disclosed. It says nothing about whether the object itself should be believed.

→ Integrity policies, on the contrary, indicate how much the object can be trusted. The policy dictates what a subject can do with that object.

For example: (i) A system administrator receives a security patch for her computer's OS. She installs it.

(ii) She is assuming that the patch came from the vendor and was not tampered with during transit.

→ She also assumes that the vendor tested the patch thoroughly.

→ She also assumes that the vendor's test environment corresponds to her environment.

* Confidentiality Policy and the Bell-Lapadula Model

→ Confidentiality Policy: also called an information flow policy, prevents the unauthorized disclosure of information

→ Unauthorized alteration of information is secondary.

→ eg. Navy should keep the date of sail secret. Redundancy systems should catch the change correctly. If the enemy knows the date of sailing, the ship could be sunk.

Bell-LaPadula Model

→ a formal model used in computer security to enforce confidentiality

→ The BLP model is based on the concept of a multilevel security system, where info. is classified into different security levels and subjects are assigned clearance levels.

→ combines mandatory and discretionary access controls

Rules

① SIMPLE CONFIDENTIALITY RULE

→ subject can only read the files at the same layer and lower levels of secrecy

→ can not read upper levels of secrecy called NO READ-UP

(2) STAR CONFIDENTIALITY RULE

→ subject can only write the files on the same level of secrecy and the upper layer of secrecy, but not the lower level of secrecy

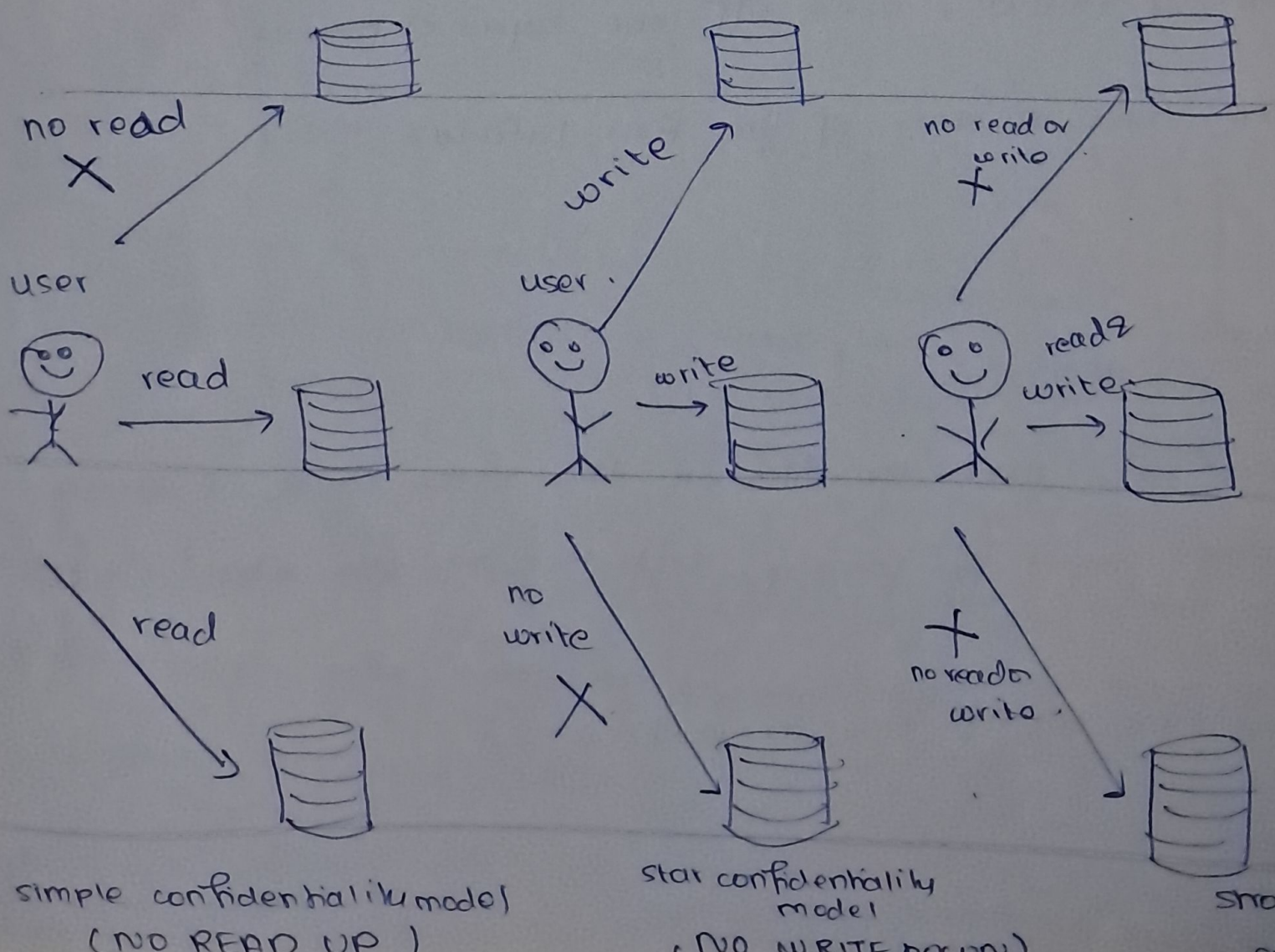
→ called as **NO WRITE DOWN**

(3) STRONG STAR CONFIDENTIALITY RULE

→ highly secure and strongest rule

→ subject can only read and write on files of the same layer, and can do no operations on the upper or lower layers of secrecy

→ called as **NO READ WRITE UP DOWN**



Star Property of Bell - LaPadula Model

Let L(S) = l_s be the security clearance of subject S

L(O) = l_o - security clearance of object O

S can write O iff $l_o \geq l_s$ and S has discretionary write access to O.

* Integrity Policies → BIBA Model
                     → Clark-Wilson Model

Biba Model

→ used to maintain the integrity of security

→ Here, the classification of subjects and objects are organized in a non-discretionary fashion, w.r.t different layers of secrecy.

→ works in the exact reverse of the Bell-LaPadula model

Rules

① SIMPLE INTEGRITY RUE

→ subject can only read the files on the same layer of secrecy and the upper layer of secrecy, but not on the lower layer of secrecy

→ called the NO READ DOWN rule

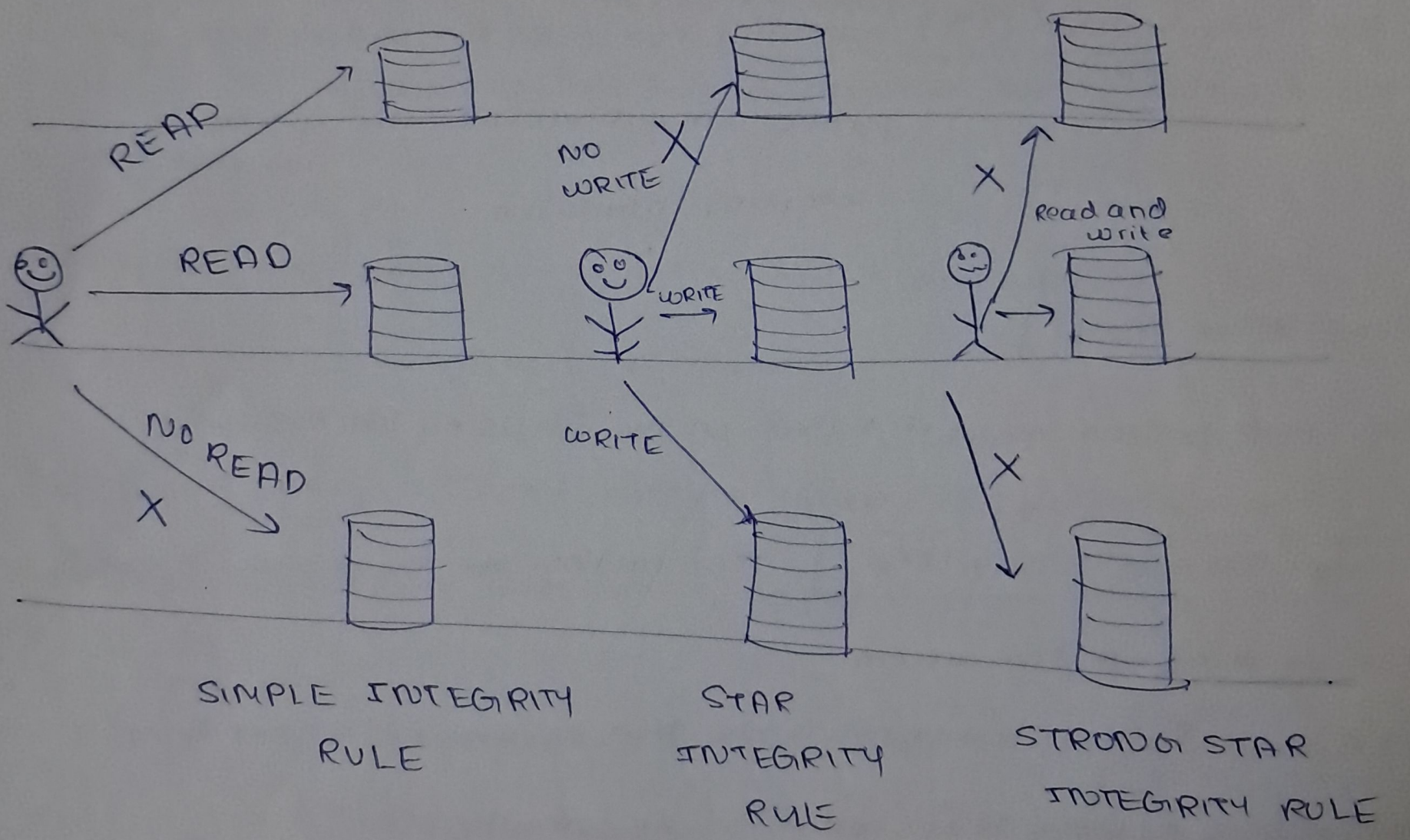
(2) STAR INTEGRITY RULE

→ 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

→ called the **NOT WRITE UP** rule.

(3) STRONG STAR INTEGRITY RULE

→ can only read and write at the same level



Note - Another rule is the Invocation Property where one can perform read, write operations on data only at their own integrity level and layer.

* Levels of Integrity

1. High Integrity Level (HI) - represents the most sensitive data eg. balance sheets and critical financial reports

2. Medium Integrity Level (LI) - includes less-critical data, such as daily transaction records

3. Low Integrity Level (LI) - contains non-sensitive data, such as public announcements and general company information

Clark Wilson Model

The Clark Wilson model is based on the following key concepts:

A. **Well-Formed Transactions** Transactions are the primary means of accessing data in the system.

→ A well-formed transaction is one that ensures the integrity and consistency of data before and after its execution

B. **Separation of Duties**

→ Different users are assigned specific roles or duties within the system.

→ These roles are designed to prevent conflicts of interest and ensure that no single user has complete control over a transaction

c. Certification and Enforcement Procedures

→ These procedures are employed so that only authorized users can perform specific actions within the system.

→ These mechanisms validate the integrity of transactions and enforce adherence to the model's principles.

Example Consider the scenario of banking operations:

Well-Formed Transactions : Before processing fund transfer, the system verifies that the customer has sufficient funds in their amount.

→ After the transaction is complete, the system updates the balances of both the sender and receiver accounts.

Separation of Duties : In the banking system, different users are assigned specific roles with distinct responsibilities. For eg.

There may be

(i) Customer Service Representatives

(ii) Transaction Approvers

(iii) System Administrators

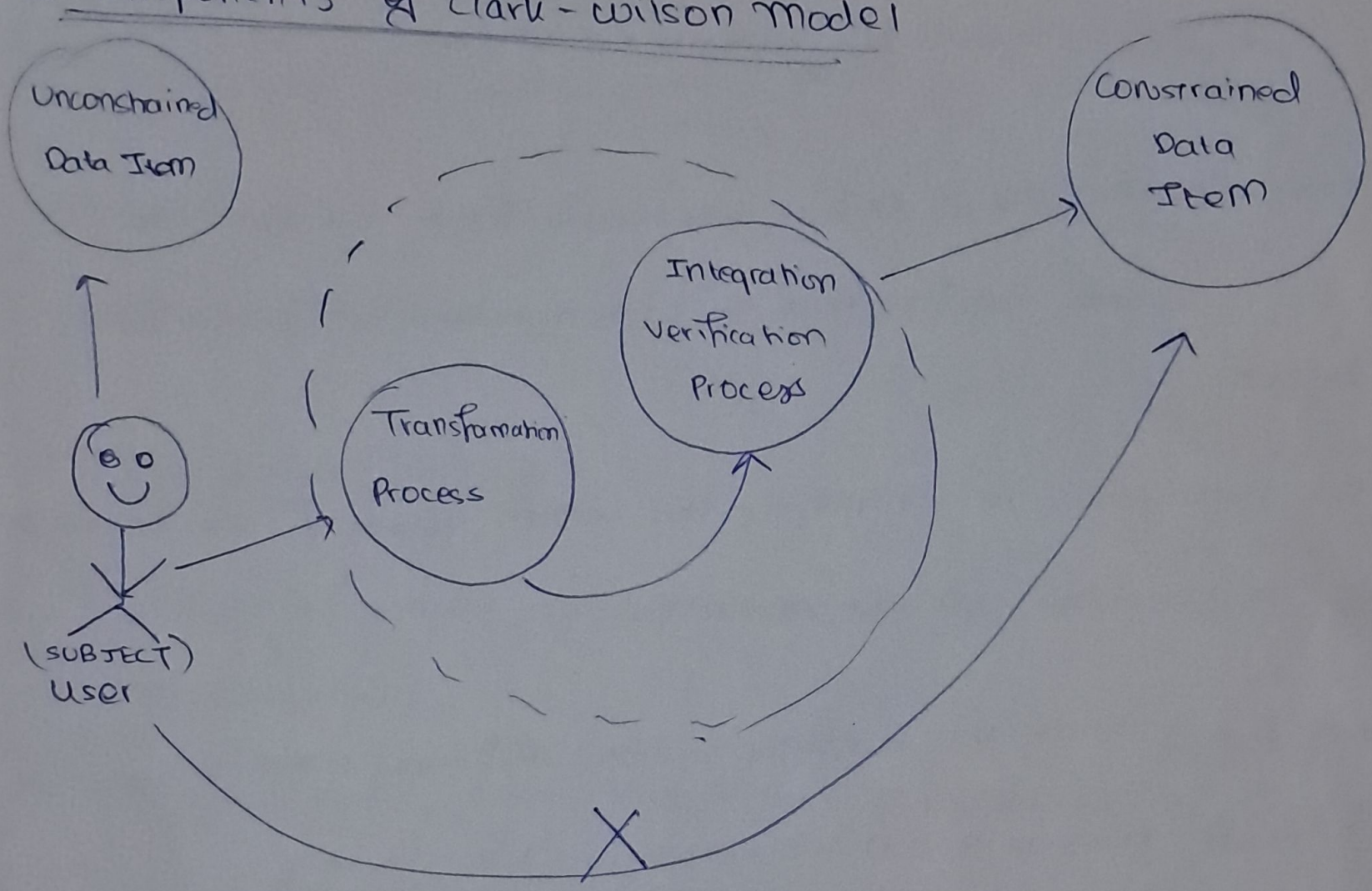
Certification and Enforcement Procedures – The system employs certain mechanisms to ensure that only authorized users can perform certain actions - eg.

→ Before a transaction is approved, it undergoes a certification

process to validate its integrity and compliance with security policies.

→ Once certified, the transaction is enforced by the system, which ensures that only authorized users can execute it and that the transaction follows the separation of duties principles.

* Components of Clark-Wilson Model



SUBJECT: Any user requesting for data items

CONSTRAINED DATA ITEMs: cannot be directly by subjects - only through Clark Wilson Model

UNCONSTRAINED DATA ITEMs: can be accessed directly by the subject

Processes

① TRANSFORMATION PROCESS - The subject's request to handle the constrained data items is handled by the transformation process which converts it into permissions and then forwards it to the Integration Verification Process.

② INTEGRATION VERIFICATION PROCESS - performs authentication and authorization, if successful, the subject is given access to the constrained data items.

* Availability Policy

→ Availability policies describe when, and for how long the resource can be accessed.

→ An availability policy ensures that a resource can be accessed in some way in a timely fashion, and promotes QoS.

→ When a resource is not available, a denial of service occurs.

→ In the general case lack of availability can be modeled using a statistical model - MTBF (Mean Time Between Failure)

* Deadlock

→ A deadlock is a state in which some set of processes block each other waiting for another process in their set to take some action.

→ Deadlock can occur if 4 conditions hold simultaneously

(i) mutual exclusion

(ii) hold and wait

(iii) no preemption

(iv) circular wait

→ There are 3 approaches to handling deadlock

(i) preventing it

(ii) avoiding it

(iii) detecting and recovering from it

* Denial of Service and Denial of Service Models

→ A denial of service occurs when a group of authorized users of a service makes that service unavailable to a disjoint group of authorized users for a period of time exceeding a defined maximum waiting time.

Security Aspects of DoS

① Physical Issues

→ The physical issues include access controls that prevent unauthorized persons from coming into contact with computing resources, hot & cold sites for use in alternative site processing

(2) Technical Issues

→ Technical issues include the fault-tolerant mechanisms, electronic vaulting (automatic backup to a secure location) and access control software to restrict unauthorized users from disrupting services.

→ Fault tolerance mechanisms involve hardware redundancy, disk mirroring and application checkpoint restart.

(3) Administrative Issues

→ The issues in the administrative aspect of availability are access control policies, operating procedures, contingency planning and user training.

→ Proper training of operators, programmers and security personnel can help avoid many computing stages that leads to the loss of availability.

DOS Failure to Release Resources

→ If an error occurs in the application that prevents the release of an in-use resource, it becomes unavailable for further resource.

eg: an application locks a file for writing but an exception occurs and the file is not unlocked

(i) use of DB connection objects where the objects are not being freed if an exception occurs

DOS Buffer Overflows

→ In languages like C, C++, where the developer has direct responsibility for managing memory allocation, buffer overflow is a risk.

⇒ For eg. if a web server has a storage of 100 bytes. An attacker can send a request to the server of 150 bytes. The buffer overflows and the 50 bytes overflow into adjacent memory areas.

Flood Attacks

→ Flood attacks occur when the system receives too much traffic for the server to manage, causing it to slow/stop

→ ICMP can send endless pings

→ SYN connection requests can be sent to the server in large amounts, but the attacker never completes the 3-way handshake.

DDos

→ In a DDOS attack, the orchestrated attack is launched from multiple locations by several systems simultaneously, whereas a DOS attack is singular in nature

* Chinese Wall Model - Hybrid Policy

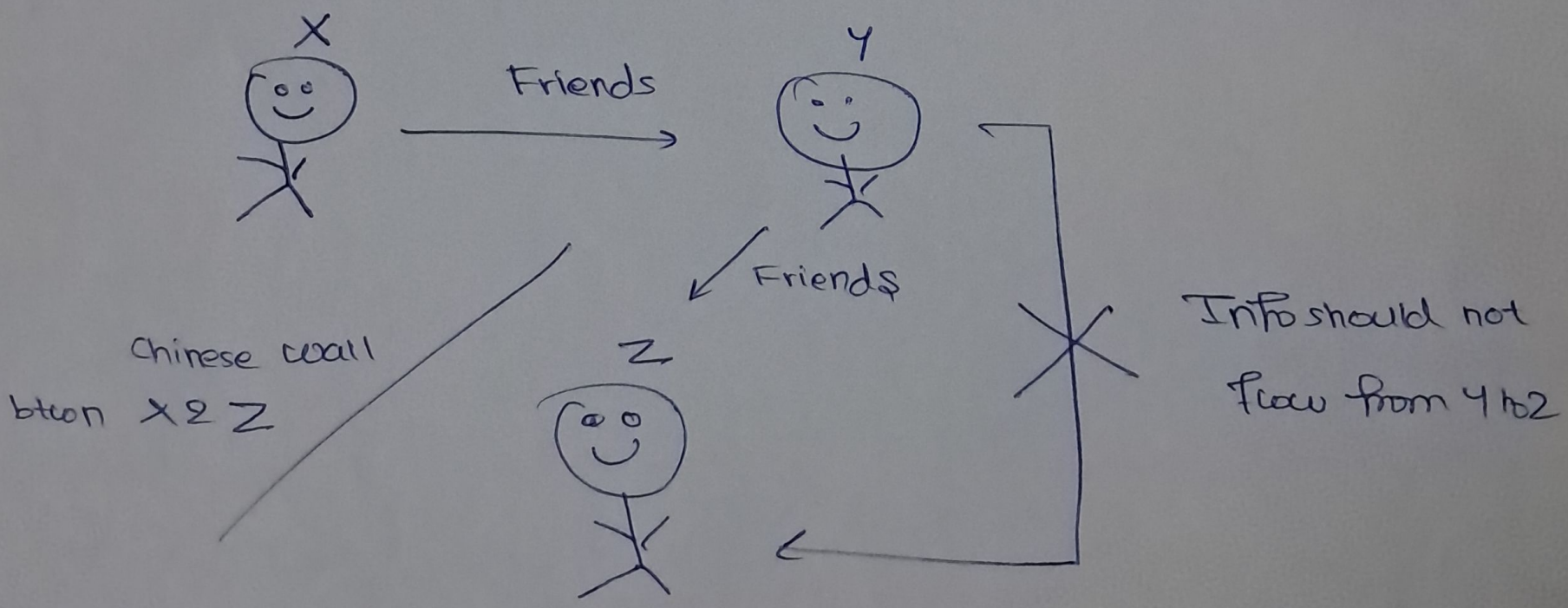
→ The Chinese Wall policy uses the concept of conflict of interest classes to implement security.

→ The companies which are in competition with each other are placed in one group.

→ This group is known as the conflict of interest class.

→ If a company tries to access an object within the same CIR class, then the access is denied.

→ Consider the following example: There are 3 people X, Y, Z.
If X and Y are friends, and also X and Z are enemies, and Y & Z are friends, confidential info of X should not go to Z via Y.



Read Rule (Simple Security Rule)

A user can read an object iff the object:

1. Belongs to the same company dataset as an object that the subject has already accessed.

(OR)

2. Belongs to a completely diff. conflict of interest class from all the objects that the subject has previously accessed.

Write Rule (Star Property)

A subject can write to an object iff

1. The subject can read the object according to the Read Rule.
2. No object in a diff. company dataset (belonging to the same conflict of interest class) has been read by the subject