Security Policies and Multilevel Security
Module 2

CSC3207 Computer Security

Outline

- Multilevel Security
- Confidentiality policies: Bell-LaPadula Model
- Integrity Policies: Biba Integrity Model, Clark-Wilson Integrity Model
- Hybrid Policies - Chinese Wall Model

References

- Chapter 9 Security Engineering: A Guide to Building Dependable Systems, 3rd Edition by Ross Anderson
- Chapter 4 Introduction to Computer Security by Matt Bishop

Multilevel Security

Multilevel Security

- a secure system should have a set of guidelines that specify the authorization of subjects to access specific objects
- "Access" implies a flow of information from a subject to an object or from an object to a subject
- For example, when a user (a subject) updates a data set (an object), the information flows from the subject to the object - When a user reads a record from a data set, the information flows from the object to the subject
- The subject in these interactions is active; the subject is attempting to access an object (or the information that the object contains)
- The object is passive; it contains the information that the subject wants to access, or it is the receiver of information from the subject
- Each time a subject attempts to access an object, the system must decide whether to allow the access

Multilevel Security

- Multilevel security is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories
- certain types of information are classified Restricted, Confidential, Secret, Top Secret
- a common protective marking scheme for the sensitivity of documents
- Classifications are labels, which run upwards from Unclassified through Confidential, Secret and Top Secret
- The original idea was that information whose compromise could cost lives was marked 'Secret' while information whose compromise could cost many lives was 'Top Secret'.
- permits access by users with different security clearances and denies access to users who lack authorization

Multilevel Security

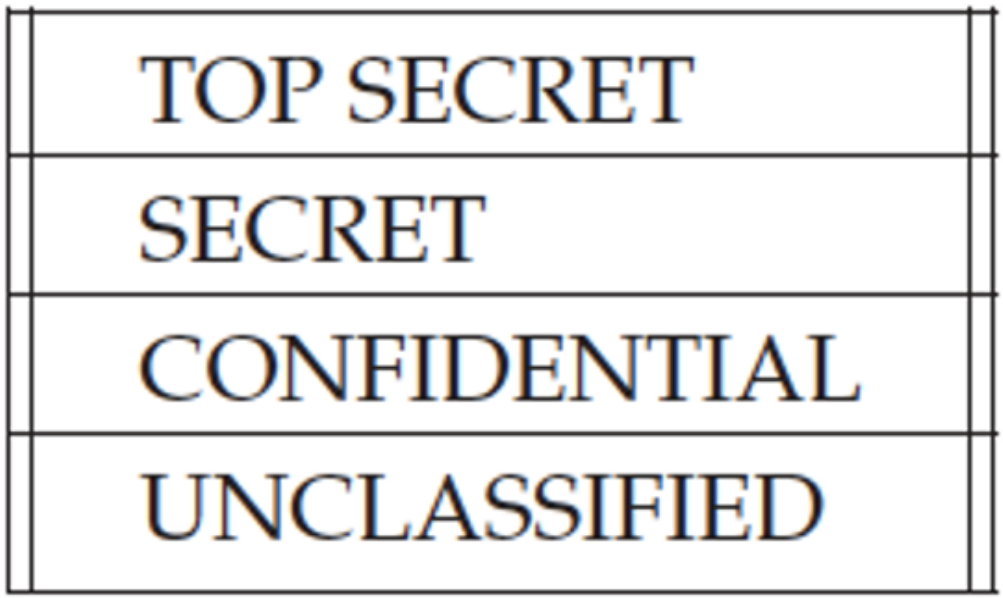


Figure 9.2: multilevel security

Multilevel Security

- The access control policy
  - you can read a document only if your clearance is at least as high as the document's classification
- So an official cleared to 'Top Secret' could read a 'Secret' document, but not vice versa
- So information may only flow upwards, from confidential to secret to top secret, but never downwards – unless an authorized person takes a deliberate decision to declassify it
- A multilevel-secure security policy has two primary goals
  - First, the controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization
  - Second, the controls must prevent individuals from declassifying information

The Bell LaPadula Model

The Bell LaPadula Model

- Is a confidentiality policy that prevents the unauthorized disclosure of information
- multilevel security policy model
- was proposed by Dave Bell and Len LaPadula
- describes a set of access control rules which use security labels on objects and clearances for subjects
- It has influenced the development of many other models and much of the development of computer security technologies
- Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public")

The Bell LaPadula Model

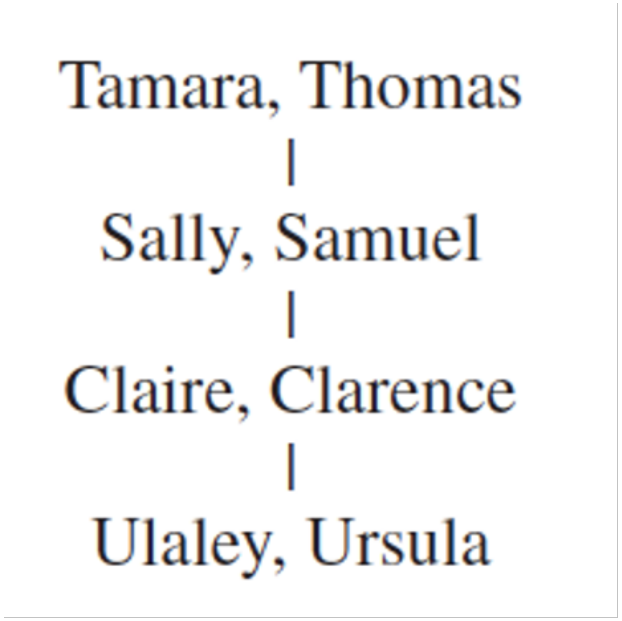
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

The Bell LaPadula Model

- the Bell-LaPadula (BLP)model enforces two properties:
  - **The simple security property**: no process may read data at a higher level
    - This is also known as no read up
    - prevents unauthorized access to sensitive information
  - **The Star Property (*-property)**: enforces the "no-write-down" rule
    - no process may write data to a lower level
    - prevents unauthorized data disclosure

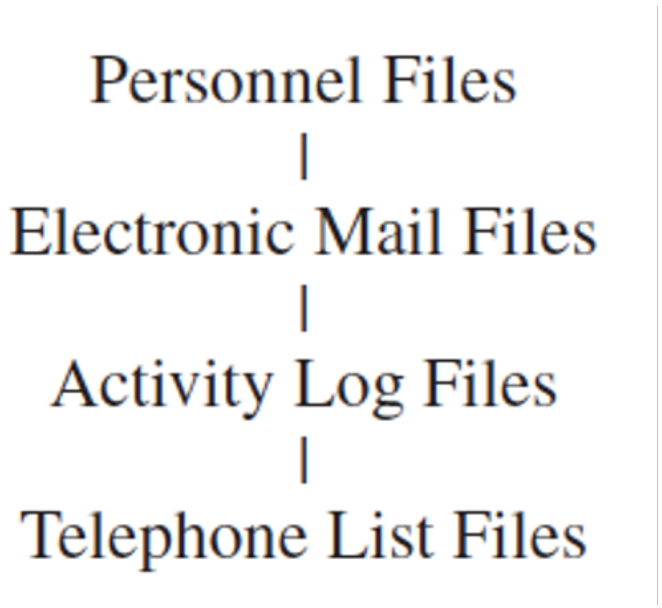
The Bell LaPadula Model

- individuals grouped by their security clearances
- A subject has a security clearance
- In the figure, Claire's security clearance is C (for CONFIDENTIAL), and Thomas' is TS (for TOP SECRET)



The Bell LaPadula Model

- a set of documents grouped by their security levels
- An object has a security classification
- the security classification of the electronic mail files is S (for SECRET), and that of the telephone list files is UC (for UNCLASSIFIED)



The Bell LaPadula Model

- When we refer to both subject clearances and object classifications, we use the term "classification."
- The goal of the Bell LaPadula security model is to prevent information flowing from objects at a security classification higher than a subject's clearance to that subject
- The Bell-LaPadula security model combines mandatory and discretionary access controls
- "S has discretionary read (write) access to O" means that the access control matrix entry for S and O corresponding to the discretionary access control component contains a read (write) right
- If the mandatory controls not present, S would be able to read (write) O

The Bell LaPadula Model

- is primarily used in military and government contexts to control access to classified information
- It forms the basis for Mandatory Access Control (MAC) in many secure operating systems
- While it is effective for enforcing confidentiality, it does not address other security aspects like integrity and availability, which may require additional security models and mechanisms

The Biba Integrity Model

The Biba Integrity Model

- For some organizations, integrity is more important than confidentiality
- security model devised in 1975 by Ken Biba
- is a formal state transition system of computer security policy describing a set of access control rules designed to ensure data integrity
- Data and subjects are grouped into ordered levels of integrity
- The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject
- deals with integrity alone and ignores confidentiality

The Biba Integrity Model

- In general the model was developed to address integrity as the core principle, which is the direct inverse of the Bell–LaPadula model which focuses on confidentiality
- confidentiality is a constraint on who can read a message, while integrity is a constraint on who can write or alter it
- was created to solve three challenges of integrity:
  - Prevent unauthorized subjects from modifying items
  - Prevent authorized people from modifying items without permission
  - Keep internal and external object consistency in mind
- Because the Biba model focuses on data integrity, it is a more common choice for commercial security models than the Bell-LaPadula model

The Biba Integrity Model

characteristic features of the Biba Model:

- Reading at a lower level violates the integrity and confidentiality of the material
- The Biba model was designed after the Bell LaPadula model to solve the issue of data integrity
- The Biba model describes states and transitions, giving priority to data integrity above confidentiality
- Because of its primary purpose of preventing unauthorized people from altering items, the Biba model quickly acquired appeal among businesses

The Biba Integrity Model

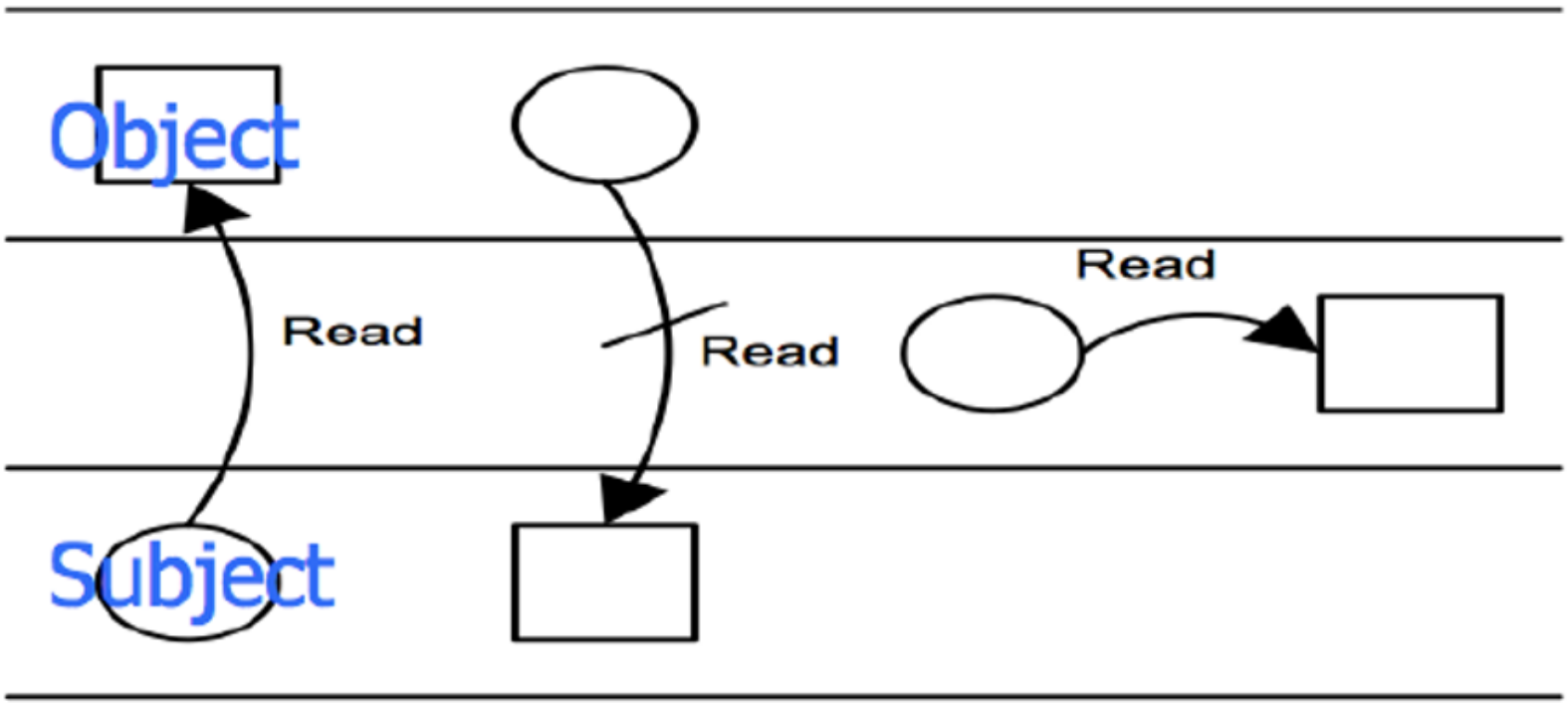
- if a general wants to change a mission that's in progress, then he has the right to do that
  - That data has a high level of integrity. Therefore, everyone below him has permission to trust that information
- if a private sends a message about a change in the mission, then that data is not to be trusted
  - It has a low level of integrity. Therefore, no one above him has permission to trust that information.

The Biba Integrity Model

- Biba utilizes the following rule: "no write up, no read down"
  - Then it enforces the rule on data (objects) and users(subject)
- The Simple Integrity Property: no read down
  - a subject cannot read an object at a lower integrity level
  - Users can not read, access, or see data one level below
- The Star (*) property: no write-up
  - Users can not create, modify, or write data of a higher level
  - a subject cannot modify an object at a higher integrity level
- invocation property: Users can not request a service of higher-level data

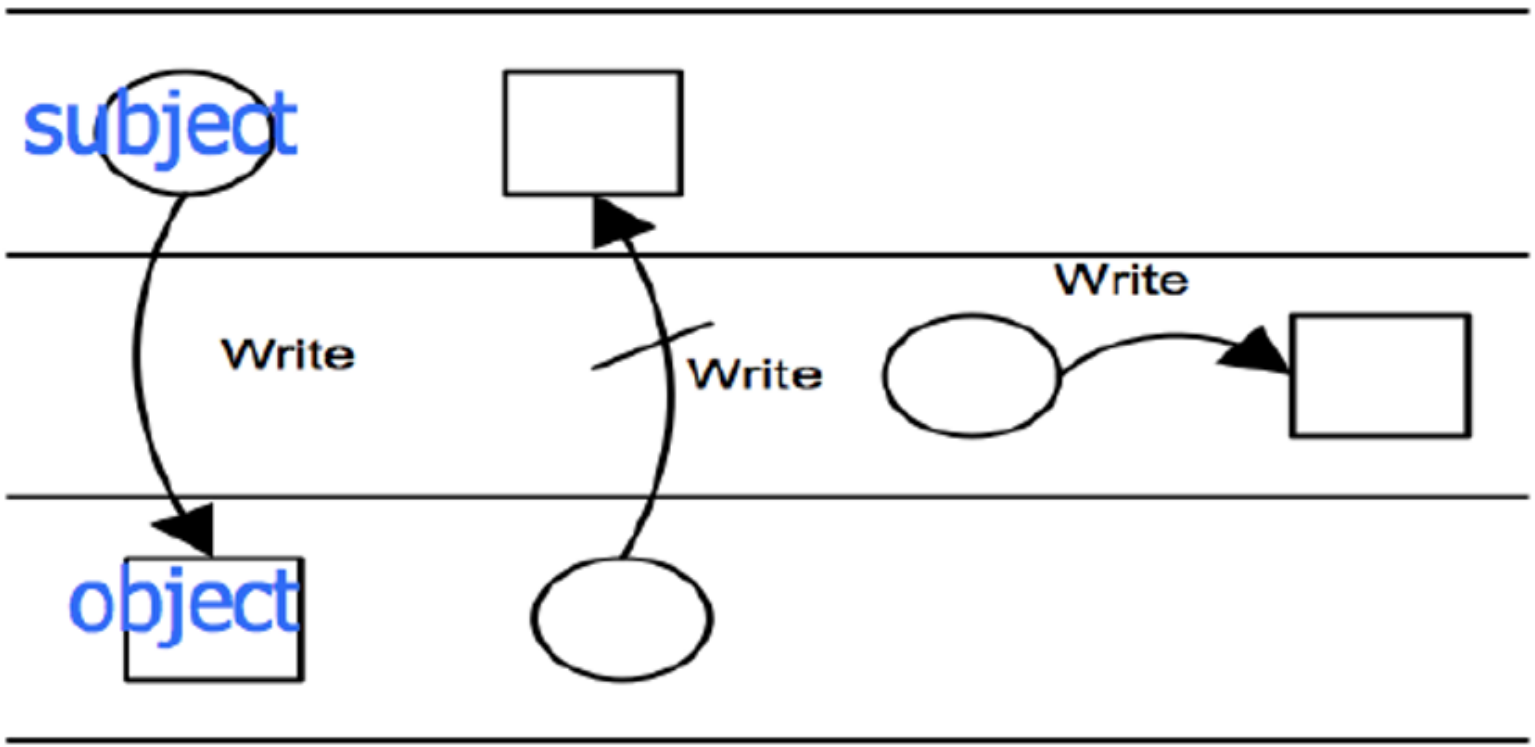
The Biba Integrity Model

- No Read Down



The Biba Integrity Model

- No Write-Up



The Clark-Wilson Integrity Model

The Clark-Wilson Integrity Model

- Instead of defining a formal state machine,the Clark-Wilson model defines each data item and allowsmodifications through only a small set of programs
- presents a methodology to specify and analyze an integrity policy for a data system.
- The chief concern of this model is the formalizing of a notion of information integrity through the prevention of data corruption in a system as a result of either faults or malicious purposes
- An integrity policy depicts the method to be used by the data items in the system in order to remain valid as they are transitioned from one system state to another
- The model stipulates the capabilities of those principals deployed within the system and the model delineates certification and enforcement rules

The Clark-Wilson Integrity Model

- uses a three-part relationship of subject/program/object (or subject/transaction/object) known as a triple or an access control triple
- Subjects do not have direct access to objects
- Objects can be accessed only through programs
- Through the use of two principles—well-formed transactions and separation of duties—the Clark-Wilson model provides an effective means to protect integrity
- A subject is able to access objects only by using a program, interface, or access portal
- Each program has specific limitations on what it can and cannot do to an object (such as a database or other resource)

The Clark-Wilson Integrity Model

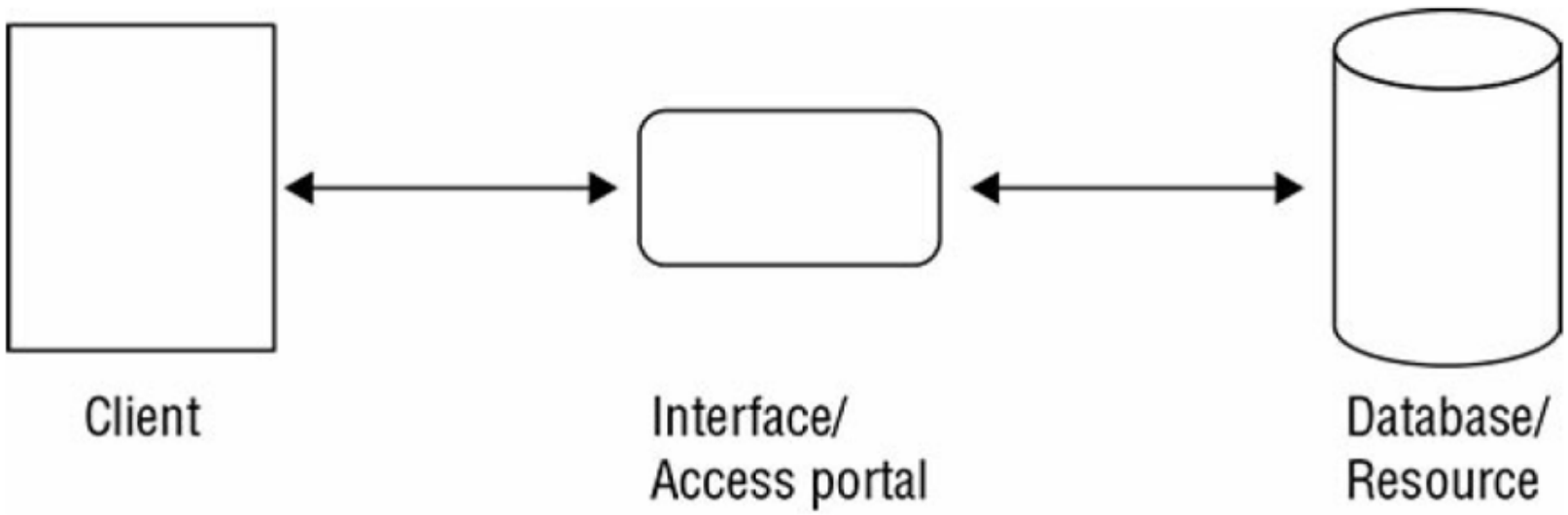


FIGURE 8.5 The Clark-Wilson model

The Clark-Wilson Integrity Model

Clark-Wilson defines the following items and procedures:

- A constrained data item (CDI) is any data item whose integrity is protected by the security model
- An unconstrained data item (UDI) is any data item that is not controlled by the security model
  - Any data that is to be input and hasn't been validated, or any output, would be considered an unconstrained data item
- An integrity verification procedure (IVP) is a procedure that scans data items and confirms their integrity
- Transformation procedures (TPs) are the only procedures that are allowed to modify a CDI
  - The limited access to CDIs through TPs forms the backbone of the Clark-Wilson integrity model

The Clark-Wilson Integrity Model

- The Clark-Wilson model uses security labels to grant access to objects,but only through transformation procedures and a restricted interface model
- A restricted interface model uses classification-based restrictions to offer only subject-specific authorized information and functions
- One subject at one classification level will see one set of data and have access to one set of functions, whereas another subject at a different classification level will see a different set of data and have access to a different set of functions

The Clark-Wilson Integrity Model

- The different functions made available to different levels or classes of users may be implemented by either showing all functions to all users but disabling those that are not authorized for a specific user or by showing only those functions granted to a specific user
- Through these mechanisms, the Clark-Wilson model ensures that data is protected from unauthorized changes from any user
- In effect, the Clark-Wilson model enforces separation of duties

The Chinese Wall Model

The Chinese Wall Model

- Combines integrity and confidentiality thus is a hybrid policy
- Also known as the Brewer and Nash model was created to permit access controls to change dynamically based on a user's previous activity making it a kind of state machine model as well
- This model applies to a single integrated database
- it seeks to create security domains that are sensitive to the notion of conflict of interest
  - for example, someone who works at Company C who has access to proprietary data for Company A should not also be allowed access to similar data for Company B if those two companies compete with each other

The Chinese Wall Model

- Organize entities into "conflict of interest" classes
- Control subject accesses to each class
- Control writing to all classes to ensure information is not passed along in violation of rules
- Allow sanitized data to be viewed by everyone

The Chinese Wall Model

- known as the Chinese Wall model because it creates a class of data that defines which security domains are potentially in conflict and prevents any subject with access to one domain that belongs to a specific conflict class from accessing any other domain that belongs to the same conflict class
- Metaphorically, this puts a wall around all other information in any conflict class
- This model also uses the principle of data isolation within each conflict class to keep users out of potential conflict-of-interest situations
- Because company relationships change all the time, dynamic updates to members of and definitions for conflict classes are important

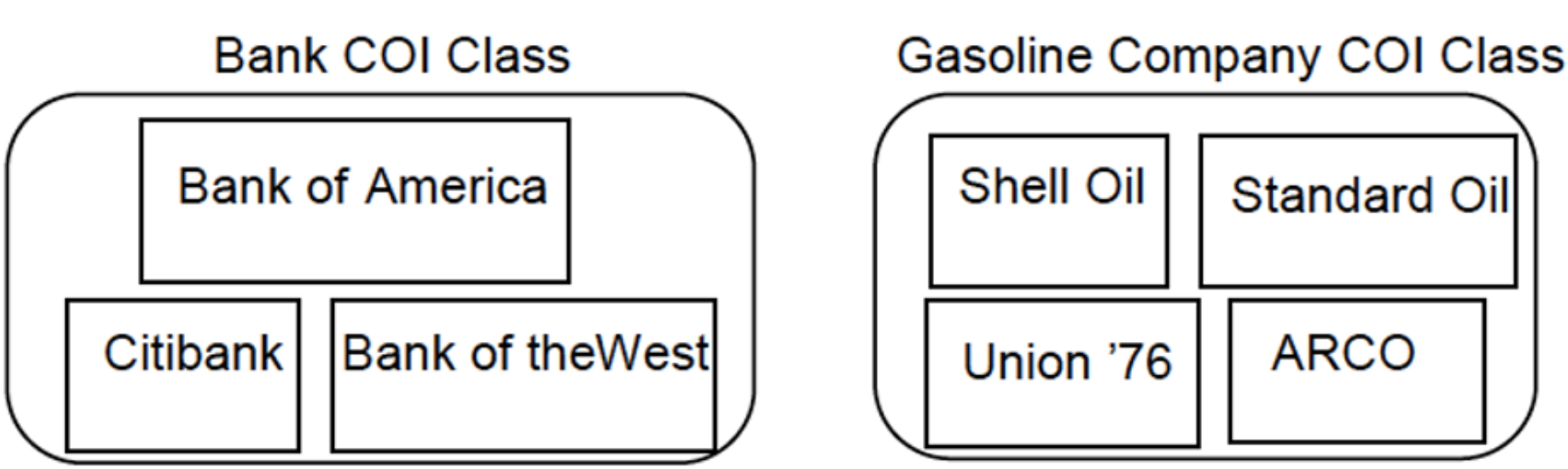
The Chinese Wall Model

- Another way of looking at or thinking of the Chinese wall model is of an administrator having full control access to a wide range of data in a system based on their assigned job responsibilities and work tasks
- However, at the moment an action is taken against any data item, the administrator's access to any conflicting data items is temporarily blocked
- Only data items that relate to the initial data item can be accessed during the operation
- Once the task is completed, the administrator's access returns to full control

The Chinese Wall Model

- Example: Consultant Kakeeto advises Stanbic Bank and Centenary Bank about investments
- Conflict of interest: advice for either bank would affect advice to the other bank
- Solution: Consultant Kakeeto can only access objects on his/her side of the wall

The Chinese Wall Model



Discussion Questions

- Compare and contrast
  - the Bell LaPadula and Biba models
  - the Biba and the Clark-Wilson integrity models
  - the Chinese Wall Policy to the Bell LaPadula and Clark-Wilson models
- What are the cons and pros of each model discussed?

Questions

What is the best definition of a security model?

A. A security model states policies an organization must follow.

B. A security model provides a framework to implement a security policy.

C. A security model is a technical evaluation of each part of a computer system to assess its concordance with security standards.

D. A security model is the process of formal acceptance of a certified configuration.

Questions

Which security model addresses data confidentiality?

A. Bell-LaPadula

B. Biba

C. Clark-Wilson

D. Brewer and Nash

Questions

Which Bell-LaPadula property keeps lower-level subjects from accessing objects with a higher security level?

A. (star) Security Property

B. No write up property

C. No read up property

D. No read down property

Questions

What is the implied meaning of the simple property of Biba?

A. Write down
B. Read up
C. No write up
D. No read down

Questions

When a trusted subject violates the star property of Bell-LaPadula in order to write an object into a lower level, what valid operation could be taking place?

A. Perturbation

B. Polyinstantiation

C. Aggregation

D. Declassification

Questions

Which of the following is not part of the access control relationship of the Clark-Wilson model?

A. Object

B. Interface

C. Programming language

D. Subject