# Computer Security (COM-301)

Mandatory Access Control

# MAC question

Which of the following statements are **true**:

a) The Chinese wall model is a form of discretionary access control.
b) For labels Unclassified < Secret < Top Secret: Level (S, {Finances, Software}) dominates Level (U,{Hardware})
c) The Bell-LaPadula (BLP) model is used to protect the confidentiality of objects.
d) The BIBA model is used to protect the integrity of objects.

Only (c) and (d) are correct. (a) The Chinese wall model is part of the BIBA model. (b) There is no relationship between these two levels.

## Mixing models

To protect both the integrity and the confidentiality of the assets in your system, you decide to establish policies following both BIBA and BLP security models setting the same integrity and confidentiality security levels. As a result:

a) All subjects can read files on security levels that dominate them
b) Subjects can read only within their own security level
c) Subjects can read and write only within their own security level
d) No subject can read or edit any files

(c)
BLP implies that subjects cannot read above their level, and cannot write below
BIBA implies that subjects cannot read below their level, and cannot write above

As a result subjects can only read and write in their own level.

# Respecting Chinese Wall

Assume two Conflict of Interest classes COI1={C1, C2, C3} and COI2={C4, C5, C6}

Assume that you have a consultancy firm. Consultancy services may involve read, write or both accesses to the company dataset. Consider the following requirements:

- Providing consulting services to C1 requires read and write access to C1 records.
- Providing consulting services to C2 requires read access to C2 records.
- Providing consulting services to C3 requires read and write access to C3 records.
- Providing consulting services to C4 requires read and write access to C4 records.
- Providing consulting services to C5 requires read access to C5 records.
- Providing consulting services to C6 requires read access to C6 records.

What is the minimum number of consultants you would need to ensure that you provide consultancy services to the six companies as per the Chinese Wall model? Show the consultant to company assignments.

**Case 1**: assume read and write are equally important for establishing an information flow.

We have two sets of conflicts.

How can we assign employees?

Employee A -> C1, implies that A cannot work with C2, C3.
Employee A -> C1, C4, implies that A cannot work with C2, C3, C5, C6 -> need another employee
Employee B -> C2, implies that B cannot work with C1, C3.
Employee B -> C2, C5, implies that B cannot work with C1, C3, C4, C6 -> need another employee
Employee C -> C3, C6

Need 3 employees, minimum.

**Case 2**: only reading is not enough to establish an information flow. Information flow

from CX to CY only happens if an employee that can read CX, can write on CY.

In this case, an employee that works on C1 or C3 cannot work on C2; and an employee that works on C4 cannot work for C5 and C6.

Employee A -> C1, implies that A cannot work with C2,C3.
Employee A -> C1, C4, implies that A cannot work with C2, C3, C5, C6 -> need another employee
Employee B -> C3, implies that B cannot work with C1, C2.
Employee B -> C3, C5, implies that B cannot work with C1, C2, C4 but can work with C6. -> need another employee
Employee C -> C2

Need 3 employees, minimum.

## Secret lovers

David and Robert are co-workers. They have started dating and they don't want the people in their office to know about their relationship, including the system administrators that inspect the network traffic and the corporate email server to avoid information leaks. What is a good covert channel to agree on the time for their next date:

a) Send the meeting time in a message on Dropbox
b) Write the meeting time on the door of the restroom
c) Encode the meeting time in whitespaces added to the corporate emails they send to each other for work
d) Send the meeting time in an encrypted corporate email



(c) Writing the meeting time in whitespaces.

All other answers are communicating via channels that are not **covert.**

## Migoop

You are hired by Migoop, a new supermarket, to build their accounting system.

The system should take in the daily cash count reported by its cashiers. The reported data is then used by Managers to produce monthly balance reports and by Accountants to audit the daily earnings.

Migoop Managers are worried about malicious cashiers reporting a wrong cash count and corrupting their monthly balance.

Explain this scenario in terms of the Biba model and assign security levels to principals and objects. Explain how the Biba rules can prevent the harms that Migoop is worried about.

Hint: Principals are the subjects in the system that can perform actions on objects. Assume that the system only covers elements mentioned in the question.

**Principals**: Manager, Accountant, Cashier
**Objects**: daily cash count, monthly balance, daily earnings

***BIBA***

| | |
|---|---|
| **Principals**: | Cashier is low level and Manager/Accountant are high level |
| **Objects** | Cash count is low level. Monthly balance/daily earnings high level |

BIBA rules impose a no-write up and no-read down policy.
In this scenario, this means that the input from a low level principal (Cashier, cash count) should not get to the high level (Manager, monthly balance) without sanitization; and that the Managers and Accountants should not look at the cash count, so as to not pollute their perception about the balance.

Sanitization in this scenario means, that the system should flag, and potentially remove, any obvious outliers (Input that is all zeros for an entire day/Suddenly selling 500 bananas per hour) from the cash counts reported by Cashiers before Managers/Accountants use the data for their reporting.