Computer Security (COM-301)

Mandatory Access Control

Interactive Exercises

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.**

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.

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 and Accountant are high level
Objects Cash count is low level. Monthly balance and 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) cannot get to the high level (Manager, monthly balance).
In class you have seen a useful tool to "lift" a low level object to a high level object: sanitization. For cash count, sanitization means that the system should allow only counts reported by Cashiers with expected formats to be upgraded, e.g., cash count is not all zeros for an entire day, the rates are reasonable (suddenly selling 500 bananas per hour is not reasonable) before Managers/Accountants use the data for their reporting. Yet, the Managers and Accountants should not look at the cash count, so as to not pollute their perception about the balance.