Homework 7: Mandatory Access Control

1. Mandatory Access Control

(a) [False] In MAC, resource owners can override system policy and allow other users access to his resources when the system forbids it.

In MAC, access control is executed at the system level. Users can't change their own security clearance or that of any resource they own. If the system denies access, that decision has to be obeyed.

(b) What is the principle of tranquility? Which principle supports least privilege better, strong tranquility or weak tranquility?

Principle of tranquility states the security clearances of subjects and objects should rarely change (never change in strong tranquility).

Weak tranquility supports least privilege better, because all subjects can start with the lowest clearance and gain access as needs require.

2. Bell-LaPadula model

(a) An idiom in the BLP model is "no read up, no write down". What does "write" mean here?
It means append, or write extra data into a file without reading or modifying existing content.

(b) Why don't we allow subjects with higher clearance to write into files with lower clearance?

This will provide a path for leaking secrets: Alice can read a secret then write it to a public file, essentially declassifying the secret.

BLP model supports "trusted subjects", who are not restrained by the "no write down" rule (*-property).

(c) Explain the following concepts in the BLP model:

- ss-property: simple security property. "No read up".
- *-property: "no write down".
- ds-property: discretionary security property. Resource owner can deny access when the system allows it. Note that if the system denies access, user can't allow it!

The textbook provides an interesting anecdote on the name "*-property", in a footnote.

(d) Here are some subjects and objects in a BLP-modeled MAC system. Bigger number means higher clearance (5 = top secret, 1 = unclassified).

Subject	Clearance
Alice	3
Bob	2
Charlie	5
Dave	1

Object	Clearance
X	4
Y	5
Z	3
W	1

Task: fill in the access rights each subject has on each object (read, write, read+write, or no access). Remember "write" doesn't imply "read" in BLP model.

	X	Y	Z	W
Alice	w	w	r/w	r
Bob	w	w	w	r
Charlie	r	r/w	r	r
Dave	w	w	w	r/w

4. Other MAC models

(a) For each of the MAC models below, decide its security focus: confidentiality, integrity, or conflict of interest?

- (confidentiality) BLP Model
- (integrity) Biba Model
- (conflict of interest) Chinese Wall Model
- (integrity) Clark-Wilson Model

(b) **Chinese Wall Model**: There are two banks (B_1, B_2), three cable companies (C_1, C_2, C_3) and four factories (F_1, F_2, F_3, F_4) in town, which form 9 datasets and 3 conflict of interest classes. Here are some facts:

- Alice can read objects in B_1 and C_2
- Bob can read objects in C_1 and F_2
- Charlie can read objects in F_4

Questions:

- Can Alice be granted read access to objects in C_3? No – conflict of interest.
- Can Bob be granted read access to objects in B_2? Yes – Bob doesn't have access to any Bank databases.
- Can Bob write into any object in C_1? No – Bob can read across two CoI classes.
- Can Charlie write into any object in F_4? Yes – Charlie only has access to one database.