**DSCI-519 Homework 2**

This is an INDIVIDUAL assignment. You may discuss it with other students, but each student must submit their own work. Prepare a report in PDF format with a font size of 10 points, single-spaced, single column (five pages maximum). Quality of your answers and analysis is more important than the quantity of words used! Submit the report on the D2L.

**Problem 1 (30 points)**

1. [10 points] Briefly describe one property that we can analyze using an Access Control Matrix but not using the Take‐Grant Model.
2. [10 points] Briefly describe one property that we can analyze using the Take‐Grant protection model but not using an Access Control Matrix.
3. [10 points] We use HRU to determine if a protection system is “safe", that is, no right is leaked. Briefly describe what we would mean by “safe" when using HRU to evaluate if a system satisfies Bell-LaPadula properties. This exercise asks you to apply the HRU method to reason about safety in BLP. You need to explicitly state what "safe" or "inability to leak a right" means in this case.

**Problem 2 (20 points)**

Consider Bel-LaPadula policy instance that contains two levels: “Top secret” and “Secret” (“Top secret” dominates “Secret”) and two categories: empty set Ø and “Europe”. Represent the Bell-LaPadula MAC rules applicable to this policy using Lampson’s Access Matrix. Note, you need to only represent simple security and \*property. This assignment asks you to draw an access control matrix that encodes the BLP rules for the given access classes.

**Problem 3 (20 points)**

In class we discussed the hardware protection ring mechanism for Multics. It consisted of three ring numbers k, l, and m that were stored in the SDW for a segment and which indicated the write, read, and execute brackets, plus the gate extension for that segment. The SDW also contained three single-bit flags to indicate the process’s access to the segment (read, write, execute), and a register that contained the current ring in which a process was executing.

1. [5 points] How do the three ring numbers define four ranges? Explain what the top and bottom of each of the brackets and gate extension are, using the ring numbers.
2. [15 points] Explain what access a process has to a segment under each of the following sets of conditions:
3. k = 4, l = 4, m = 6; read flag: on, write flag: on, execute flag: on; process current ring = 4
4. k = 0, l = 4, m = 6; read flag: on, write flag: on, execute flag: on; process current ring = 7
5. k = 4, l = 4, m = 6; read flag: on, write flag: on, execute flag: on; process current ring = 3
6. k = 0, l = 4, m = 6; read flag: on, write flag: on, execute flag: off; process current ring = 6
7. k = 0, l = 4, m = 6; read flag: on, write flag: on, execute flag: on; process current ring = 5

**Problem 4 (30 points)**

As discussed in class, different system users in Lipner model must be able to perform the following:

1. Ordinary users can execute (read) production code but cannot alter it
2. Ordinary users can alter and read production data
3. System managers need access to all logs but cannot change levels of objects
4. System controllers need to install code (hence downgrade capability)
5. Subjects need to have append-only access to logs

Explain how these requirements are satisfied by the label assignment (see Lecture 7). Provide detailed explanation by showing the effects of applying BLP and Biba rules to the labels of relevant object and subject types. Use case 1 (“Ordinary users can execute (read) production code but cannot alter it”) that we discussed in class, as an example.