**DSCI-519 Homework 1**

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.

Note: this assignment is intentionally open-ended, there can be more than one correct answer. Make any relevant reasonable assumptions as you need to, just make sure to clearly state your assumptions in your report.

**Problem 1 (40 points)**

**Scenario:** You have been asked to provide advise on how a company can manage security on their customer information database. The database maintains information on customer sales contacts, orders, and pricing options. Their goal is a database that will be available to their (traveling) sales people via the Internet, to customers for reviewing orders and payment, and within the company for financial reporting, order forecasting, etc. As such, the system contains confidential information and information where integrity is critical. Your task is to identify security threats, and to choose approaches to reduce the risk. You need to explain why the techniques address the threats, and why the threats matter.

**Deliverable and Grading**: You need to describe your recommendations to the Chief Information Officer of the company. Provide a written report (2 pages max) for the CIO. This should cover:

1. What are the threats? (5 points)
2. Why the threats are important? (5 points)
3. A brief description of the threat mitigation techniques. (10 points)
4. How you would apply the proposed techniques? (10 points)
5. How the techniques would protect against the threats? (10 points)

**Problem 2 (30 points)**

**Scenario:** A cloud provider has two customers, Alice and Bob who want to store their files on the cloud and share some files with each other. There is also an Administrator to manage the accounts.

* The cloud provider (Administrator acts as a proxy for the cloud service) will make money by selling advertisements based on the contents of the users’ files.
* The user accounts are separate, although users are allowed to make specific files shareable.

**Deliverable and Grading**: Complete a written report (2 pages max) discussing the following:

1. What are some security policies that this system should enforce? Consider the access needs of the users (Alice and Bob) as well as the Administrator. (10 points)
2. Draw an access matrix that implements the policies. Use any of the access modes (read, write, execute, own) from the readings. (10 points)
3. Sketch the system and “interpret” the reference monitor (including the subjects, objects, access database, audit records). You can list the elements or draw a diagram. Just be sure to demonstrate the mapping between the entities and the RM components. (5 points)
4. What are some of the possible security mechanisms the system could use to implement the reference monitor? (5 points)

**Problem 3 (30 points)**

**Scenario:** A company has the following (abbreviated) information classification policy:

* Anyone can read public data
* Only employees and people who have signed non-disclosure agreements (NDAs) can view confidential information
* Only employees can view corporate data
* Only certain employees and managers, and designated outsiders who sign NDAs, can view “insider restricted” data
* Only high-level managers (directors and above) can view “management restricted” data
* Only C-level managers and Board members can view “board restricted” data
* Only certain employees and managers with a need-to-know can view personal employee data (HR data)
* Only certain employees and managers with a need-to-know can view accounts receivable data
* Only certain employees and managers with a need-to-know can view sensitive client data, and there are strict laws against revealing this information outside of the company

**Deliverable:** interpret this policy for computers using MAC:

* Define MAC labels (access classes) that contain levels and categories (10 points)
* Define classifications and clearances for the objects and subjects (10 points)
  + I.e., assign the labels to specific types of users and types of information to express the policy you want to enforce
* Show the *dom* relationship for your MAC labels (10 points)
* You can achieve this in two ways:

1. List dominance relationship for all possible combination of your access classes
2. Create a chart representing a hierarchy of the access classes by drawing a lattice structure (as we did in class)

* As long as you are able to convey the dominance relationship, any method is acceptable.