**Homework #3**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, March 3rd prior to class (11:59 PM)

**Homework #3 is focused on user authentication and access control. There are 10 total questions all worth 10 points each (100 pts total).**

**Chapter 3 – User Authentication**

1. In general terms, what are four means of authenticating a user’s identity? Give examples of each.
2. List and briefly describe the principal threats to the secrecy of passwords.
3. List and briefly describe four common techniques for selecting or assigning passwords.
4. List and briefly describe the principal physical characteristics used for biometric identification.
5. Assume passwords are selected from four-character combinations of 26 alphabetic characters. Assume an adversary is able to attempt passwords at the rate of one per second.

Assuming no feedback to the adversary until each attempt has been completed. What is the expected time to discover the correct password?

**Hint:** On average, only half the total possibilities need to be attempted.

**Chapter 4 – Access Control**

1. List and define the three classes of subject in an access control system.
2. Briefly define the four RBAC models of Figure 4.8a.
3. List and define the four types of entities in a base model RBAC system.
4. Describe three types of role hierarchy constraints.
5. UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?