CALIFORNIA STATE UNIVERSITY
LONG BEACH

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.

Something the individual knows. A password, PIN, or secret questions.

Something the individual possesses. An example could be physical keys.

Something the individual is. Fingerprints scan would be an example.

Something the individual does. Characteristics of the individual handwriting would be an example.

2. List and briefly describe the principal threats to the secrecy of passwords.

   Offline dictionary attack-The attacker obtains the system's password file and compares the password hashes against hashes of commonly used passwords. If the attacker finds a match, then could get access with the ID and password combination.

   Specific account attack-The attacker targets a specific account and continuously submit password guesses until the correct password is found.

   Popular password attack-attack a variety of different users but use popular password.

   Workstation hijacking-The attacker waits until a logged-in workstation is unattended.

   Exploiting users mistakes-Attack tricks the user into revealing a password.

   Exploiting multiple password use electronic monitoring-If a password is communicated across a network, it is vulnerable to eavesdropping.

3. List and briefly describe four common techniques for selecting or assigning passwords.

   1. User education

   2. Computer-generated passwords

    3. Reactive password checking-systems runs password cracker and notifies user if password has been cracked.

    4. Proactive password checking-user chooses password based on rules given by system.

4. List and briefly describe the principal physical characteristics used for biometric identification.

    a. Facial characteristics

    b. Fingerprints

    c. Hand geometry

    d. Retinal pattern

    e. Iris

    f. Signature

    g. voice

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.

    26^4 = 456976

    456976 / 2 = 228488

    228488 / 60 * 60 * 24 = 2.644 days

    2.644 days = 63.456 hours

    63.5 hours

Chapter 4 – Access Control

1. List and define the three classes of subject in an access control system.
    a. Owner-this maybe be the creator of the resource
    b. Group-group of users granted access rights
    c. Word-the latest amount of access is granted to users who are able to accesss the system but are not included in the categories owner and group of this resource
2. Briefly define the four RBAC models of Figure 4.8a.
    a. RBAC0-minimum functionality of an RBAC system.
    b. RBAC1-RBAC0 functionality and adds role hierarchies.
    c. RBAC2-RBAC0 functionality and adds constraints.
    d. RBAC3-contains functionality of all previously mentioned.
3. List and define the four types of entities in a base model RBAC system.
    a. User-An individual that has access to this computer system.
    b. Role-A named job function within the organization that controls this computer system.
    c. Permission-An approval of a particular mode of access to one or more objects.
    d. Session-A mapping between a user an activated subset of the set of roles to which the user is assigned.
4. Describe three types of role hierarchy constraints.
    a. Mutually exclusive roles are roles such a user can be assigned to only one role in the set.
    b. Cardinality refers to setting a maximum number with respect to roles.
    c. Prerequisite which allows a user to have a particular if there were already assigned to some other specified role.
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?

Suppose that we had an owner and group user that both have access to directories and files inside some directory. Suppose that an owner had rights to write to a certain file, but the group did not. A group member still has access to the directory so could delete the file and insert a new file.