**Homework #3 Answers**

**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:** Examples includes a password, a personal identification number (PIN), or answers to a prearranged set of questions.

**Something the individual possesses:** Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.

**Something the individual is (static biometrics):** Examples include recognition by fingerprint, retina, and face.

**Something the individual does (dynamic biometrics):** Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

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

We can identify the following attack strategies and countermeasures:

**Offline dictionary attack:** Typically, strong access controls are used to protect the system's password file. However, experience shows that determined hackers can frequently bypass such controls and gain access to the file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination.

**Specific account attack:** The attacker targets a specific account and submits password guesses until the correct password is discovered.

**Popular password attack:** A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs. A user's tendency is to choose a password that is easily remembered; this unfortunately makes the password easy to guess.

**Password guessing against single user:** The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.

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

**Exploiting user mistakes:** If the system assigns a password, then the user is more likely to write it down because it is difficult to remember. This situation creates the potential for an adversary to read the written password. A user may intentionally share a password, to enable a colleague to share files, for example. Also, attackers are frequently successful in obtaining passwords by using social engineering tactics that trick the user or an account manager into revealing a password. Many computer systems are shipped with preconfigured passwords for system administrators. Unless these preconfigured passwords are changed, they are easily guessed.

**Exploiting multiple password use.** Attacks can also become much more effective or damaging if different network devices share the same or a similar password for a given user.

**Electronic monitoring:** If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping. Simple encryption will not fix this problem, because the encrypted password is, in effect, the password and can be observed and reused by an adversary.

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

**User education:** Users can be told the importance of using hard-to guess passwords and can be provided with guidelines for selecting strong passwords.

**Computer-generated passwords:** the system selects a password for the user.

**Reactive password checking:** the system periodically runs its own password cracker to find guessable passwords.

**Proactive password checking:** a user can select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

1. List & briefly describe the principal physical characteristics used for biometric identification.

**Facial characteristics:** Facial characteristics are the most common means of human-to-human identification; thus, it is natural to consider them for identification by computer. The most common approach is to define characteristics based on relative location and shape of key facial

features, such as eyes, eyebrows, nose, lips, and chin shape. An alternative approach is to use an infrared camera to produce a face thermogram that correlates with the underlying vascular system in the human face.

**Fingerprints:** Fingerprints have been used as a means of identification for centuries, and the process has been systematized and automated particularly for law enforcement purposes. A fingerprint is the pattern of ridges and furrows on the surface of the fingertip. Fingerprints are

believed to be unique across the entire human population. In practice, automated fingerprint recognition and matching system extract a number of features from the fingerprint for storage as a numerical surrogate for the full fingerprint pattern.

**Hand geometry**: Hand geometry systems identify features of the hand, including shape, and lengths and widths of fingers.

**Retinal pattern:** The pattern formed by veins beneath the retinal surface is unique and therefore suitable for identification. A retinal biometric system obtains a digital image of the retinal pattern by projecting a low-intensity beam of visual or infrared light into the eye.

**Iris:** Another unique physical characteristic is the detailed structure of the iris.

**Signature:** Each individual has a unique style of handwriting and this is reflected especially in the signature, which is typically a frequently written sequence. However, multiple signature samples from a single individual will not be identical. This complicates the task of developing a

computer representation of the signature that can be matched to future samples.

**Voice:** Whereas the signature style of an individual reflects not only the unique physical attributes of the writer but also the writing habit that has developed, voice patterns are more closely tied to the physical and anatomical characteristics of the speaker. Nevertheless, there is still a variation from sample to sample over time from the same speaker, complicating the biometric recognition task.

1. 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.

T = 264/2 seconds = 63.5 hours

**Chapter 4 – Access Control**

1. List and define the three classes of subject in an access control system.

**Owner:** This may be the creator of a resource, such as a file. For system resources, ownership may belong to a system administrator. For project resources, a project administrator or leader may be assigned ownership.

**Group:** In addition to the privileges assigned to an owner, a named group of users may also be granted access rights, such that membership in the group is sufficient to exercise these access rights. In most schemes, a user may belong to multiple groups.

**World:** The least amount of access is granted to users who are able to access the system but are not included in the categories owner and group for this resource.

1. Briefly define the four RBAC models of Figure 4.8a.

RBAC0 contains the minimum functionality for an RBAC system. RBAC1 includes the RBAC0 functionality and adds role hierarchies, which enable one role to inherit permissions from another role. RBAC2 includes RBAC0 and adds constraints, which restrict the ways in which the components of a RBAC system may be configured. RBAC3 contains the functionality of RBAC0, RBAC1, and RBAC2.

1. List and define the four types of entities in a base model RBAC system.

**User:** An individual that has access to this computer system. Each individual has an associated user ID.

**Role:** A named job function within the organization that controls this computer system. Typically, associated with each role is a description of the authority and responsibility conferred on this role, and on any user who assumes this role.

**Permission:** An approval of a particular mode of access to one or more objects. Equivalent terms are access right, privilege, and authorization.

**Session:** A mapping between a user and an activated subset of the set of roles to which the user is assigned.

1. Describe three types of role hierarchy constraints.

**Mutually exclusive roles** are roles such that a user can be assigned to only one role in the set. **Cardinality** refers to setting a maximum number with respect to roles. A system might be able to specify a **prerequisite**, which dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role.

1. 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 the directory **d** and the file **f** have the same owner and group and that **f** contains the text *something*. Disregarding the superuser, no one besides the owner of **f** can change its contents can change its contents, because only the owner has write permission. However, anyone in the owner's group has write permission for **d**, so that any such person can remove **f** from **d** and install a different version, which for most purposes is the equivalent of being able to modify **f**.