Access Control and Authentication Optional Worksheet (for self study)

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.

2. What is the purpose of the password salting?

   There are two major purposes of the password salting:

   - It significantly increases the difficulty of dictionary attacks. The attacker now needs to pre-compute a hash table for each possible salt value. If the salt is l-bit long, then the attacker needs to prepare 2^l hash tables in advance.
   - It also hides the same password in the system. Without the salt, if two users have exactly the same password, the two password hashes will always be the same. If the attacker finds the password for one of these hash values, then the attacker also knows those users who use the same password in the system. With the salt, the two password hashes for the same password will be different if the salt values are distinct.

3. Answer the following questions:

   (a) What form of authentication is password-based authentication?

   (b) What are the major problems of authentication using static passwords?

(c) What are the possible solutions to improve it?

(d) What are the solutions to manage (store, maintain) passwords safely?

(a) ”Something you know” (SYK)

(b) Problems: Guessable, Forgettable, Enumerable (countable), Reusable, Re-playable, Leakable.

(c) Solutions: Multi-factor Authentication, Educating Users, Challenge and Response, User Account Management, Password Management, Password Aging, Trusted Third Party.

(d) Password Management Solution: password hashing, password aging, Never create an account without password, Keep an eye on inactive accounts

4. What is ”one time password” How does it apply in Internet banking?

   Short time or One-off password. Normally generated by a token or sent via SMS using mobile phone as a second-factor of authentication.

5. In the context of biometric user authentication, explain the terms, enrolment, verification, and identification.

   Enrolment: is analogous to assigning a password to a user. For a biometric system, the user presents a name and, typically, some type of password or PIN to the system. At the same time the system senses some biometric characteristic of this user (e.g., fingerprint of right index finger). The system digitizes the input and then extracts a set of features that can be stored as a number or set of numbers representing this unique biometric characteristic; this set of numbers is referred to as the user’s template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value.

   Verification is analogous to a user logging on to a system by using a memory card or smart card coupled with a password or PIN. For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user.

   For an identification system, the individual uses the biometric sensor but presents no additional information. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified, otherwise, the user is rejected.