FIT2093: Tutorial 2 sample solutions

Authentication

Review Questions

1. In general terms what are the three means of authenticating a user's identity?
   - Something you know: password, pin code…
   - Something you have: smart-card, ATM, phone number…
   - Something you are: fingerprint, iris …
   - In some documents, another form of authentication named "something you do" is added. It is referred to authentication using "signature, voice recognition, pin pressing pattern (the speed and power when you press pin code into pin pad)"
2. 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.

3. Explain the difference between a simple memory card and a smart card.

   Memory cards can store but not process data. Smart cards have a microprocessor.

4. 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

5. Define the terms *false match rate* and *false nonmatch rate,* and explain the use of a threshold in relationship to these two rates.
    - A false match occurs when an imposter's biometric data is declared by the system to be matched with the stored biometric data for a user.
    - A false mismatch occurs when the system declares that the biometric data of a genuine user does not match the stored biometric data for that user.
    - The rate refers to the probability of a false match or false mismatch.
    - If the matching score of the presented value, $S \geq T$ (a threshold) then a match is assumed and for $S < T$, a mismatch is assumed.
6. Describe the general concept of a challenge-response protocol.
    In general terms, a challenge-response protocol functions as follows: A user attempts to logon to a server. The server issues some sort of challenge that the user must respond to in order to be authenticated.

7. What is meant by a one-way hash function? Why is it useful in security functions and or protocols?

   A function f that is easy to calculate in one direction ($x \rightarrow f(x)$) and infeasible in the opposite direction ($f(x) \rightarrow x$).

   It can be used to turn data into smaller format that is infeasible to find the reverse (in theory). It is computationally infeasible (in practice) to derive the data from its derivation.

   A (cryptographically strong) one-way hash function is normally used as part of some security functions/protocols e.g. in generating the digital signature of a message. Another example is to transform the passwords and storing them in a shadow file so that it is difficult for the hackers and adversaries to compute the password from the hash value.

8. Answer the following questions:
   a. What form of authentication uses passwords?
   b. What are the major problems for authentication using static password?
   c. What are the possible solutions to improve it?
   d. What are the solutions to manage (store, maintain) passwords safely?

   a. "Something you know"
   b. Problems:
      - Guessable, Forgettable, Enumerable (countable), Reusable, Re-playable, Leakable.
   c. Solutions: Educating Users, Challenge and Response, User Account Management, Password Management, Password Aging, Trusted Third Party.
   d. Password Management Solution:
      - Scramble password (hash, encrypt password), password aging, never create an account without password, keep an eye on inactive accounts

9. 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.

Problems

1. Let *x* to be a password that contains exactly 3 characters. The characters are chosen from a set of alphabet A={a,b,c,d,e}. How many possible distinct *x* can be created.
    a. If *x* can contain repeated characters? i.e aaa is a valid password
    $5^3 = 125$
    b. If *x* should not contain repeated characters? i.e aab is not a valid password
    5*4*3 = 60

2. Following from previous question. A new set of alphabet B={1,2} has been added to the system. How many possible of distinct ***x*** can be created?
    a. If the following rules to be followed as a system rule:
        - The characters for the password can be chosen from A, B or both, and.
        - The characters can be repeated, and
        - There is no restriction on the minimum number of characters to be taken from each alphabet., ie aaa is a valid password.

    ANS: 7^3
    b. If the following rules to be followed as a system rule:
        - The characters for the password can be chosen from A, B or both, and
        - The characters CANNOT be repeated, and
        - There is no restriction on the minimum number of characters to be taken from the alphabets., ie abc is a valid password.

    ANS: 7*6*5
    c. If the following rules to be followed as a system rule:
        - The characters for the password should be chosen at least one character from A and one character from B, and
        - The characters can be repeated.

ANS: 7^3 - 5^3 - 2^3 (set of all possible password – sets of illegal passwords)

3. Using the observation from the results of calculations in questions 1 and 2 above, what can be said about:
    a. The total number of potential attempts one has to perform to crack a password in relation to the alphabet size? i.e will the number of attempts decrease if we decrease the alphabet size?

       The number of possible passwords will increase with the increase both in the number of alphabets used as well as the length of the password – however in the latter case the number of password will increase exponentially (due to the length of the password as the power of the number of alphabets).
    b. The total number of potential attempts that one has to perform to crack a password in relation to the alphabet type? i.e will the number of attempts decrease if we use multiple types (letter and digit) and there is a requirement to use at least one member of each alphabet type?

       Most crackers do not attempt the exhaustive approach (brute-force), rather they generate a subset of potential password based on knowledge how user create their passwords in the first place. Under this assumption, it will make the life a cracker harder if the password chooses letters from different alphabet types.
4. Consider the rules of generating password in question 2. Which set of rules will generate the highest amount of distinct passwords?

   Just look at the number of distinct number of passwords in question 2.
5. Which set of rules would you consider to be the best policy for password management that ensures high security to the system?

   From the security point of view, longer passwords with letters chosen from different alphabet types so as to reduce the chance of random or limited guessing of the password.
6. Explain the suitability or unsuitability of the following passwords:
    a. YK334 : If this is a license plate number, that is easily guessable.

b. mfmitm (for " my favourite movie is tender mercies") : suitable
c. Natalie1 : easily guessable
d. Washington : easily guessable
e. Aristotle : easily guessable
f. tv9stove : suitable
g. 12345678 : very unsuitable
h. dribgib : This is bigbird in reverse; not suitable.

7. Assume passwords are selected from four-character combinations of 26 alphanumeric characters. Assume that an adversary is able to attempt passwords at a rate of one per second.
   a. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

      $$T = (\frac{26^4}{2}) \sec onds = 63.5 hours$$

   b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

      Expect 13 tries for each digit. T = 13 x 4 = 52 seconds.

8. Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 10 characters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions per second. How long will it take to test exhaustively all possible passwords on a UNIX system?

   There are $95^{10} \approx 6 \times 10^{19}$ possible passwords. The time required is:

   $$\frac{6 \times 10^{19} passwords}{6.4 \times 10^6 passwords / \sec ond} = 9.4 \times 10^{12} \sec onds = 300{,}000 years$$