FIT2093: Tutorial 2

Authentication

Review Questions

1. In general terms what are the three means of authenticating a user's identity?
2. List and briefly describe the principal threats to the secrecy of passwords.
3. Explain the difference between a simple memory card and a smart card.
4. In the context of biometric user authentication, explain the terms, enrolment, verification, and identification.
5. Define the terms *false match rate* and *false nonmatch rate,* and explain the use of a threshold in relation to these two rates.
6. Describe the general concept of a challenge-response protocol.
7. What is meant by a one-way hash function? Why is it useful in security functions and or protocols?
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?
9. What is "one-time password"? How does it apply in internet banking?

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

   b. If *x* should not contain repeated characters? i.e aab is not a valid password

2. Following from the 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 are 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.
   b. If the following rules are 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.
   c. If the following rules to be followed as a system rule:
      - the characters for the password should be chosen such that at least one character is from A and one character is from B, and
      - the characters can be repeated.

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?
   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?

4. Consider the rules of generating password in question 2.
    a. Which set of rules will generate the highest amount of distinct passwords?
5. Which set of rules would you consider to be the best policy for password management that ensures high security to the system?
6. Explain the suitability or unsuitability of the following passwords:
    a. YK334
    b. mfmitm (for “ my favourite movie is tender mercies”)
    c. Natalie1
    d. Washington
    e. Aristotle
    f. tv9stove
    g. 12345678
    h. dribgib
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?
    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?
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?