Review Question Chapter 3

3.8) Define the terms *false match rate* and *false nonmatch rate*, and explain the use of a threshold in relationship to these two rates

Operation of Biometric Authentication System

The individual uses the biometric sensor of system maps to physical characteristic of the individual into a digital representation. For each individual, a single digital representation, or template, is stored in the computer. The system compares the stored template to the presented template. There might not be an exact match between the two templates of the user because of complexities of physical characteristics so we cannot expect it.

Thus, the system uses an algorithm to generate a matching score based off the similarities between the input and the stored templates.

This matching score varies for the same user when testing several different times.

**False match rate:**

Is the frequency (probability) that when biometric data of an imposter matches with the biometric data of a user, meaning that biometric samples from different sources are assessed to be from the same source.

**False mismatch rate:**

Is the frequency (probability) that when biometric data does not match with the biometric data of that user, meaning that samples from the same source are assessed to be from different sources.

**Use of a threshold:**

* A threshold value **t** is picked to identify the false match and the false nonmatch
* A threshold value is selected thus that if the presented value s ≥ t then a match is assumed
* A threshold value s < t, then a mismatch is assumed
* Based on the Figure 3.10 in textbook, the shaded part to the right of **t** indicates a range of values for which is false match is possible, and the other side indicates false mismatch is possible. By moving the threshold, left or right, the probabilities can be altered, but note that a decrease in false match rate results in an increase in false nonmatch rate, and vice versa.

Problems Chapter 3

3.8)

(A **salt** is [random](https://en.wikipedia.org/wiki/Random_Number_Generator) data that is used as an additional input to a [one-way function](https://en.wikipedia.org/wiki/One-way_function) that "[hashes](https://en.wikipedia.org/wiki/Cryptographic_hash_function)" [data](https://en.wikipedia.org/wiki/Data_(computing)), a [password](https://en.wikipedia.org/wiki/Password) or [passphrase](https://en.wikipedia.org/wiki/Passphrase))

The attacker can guess the password and encrypt easily if the password is not protected with salt. For example, if the password file is protected with the salt, the attacker need to guess the password and encrypt in once for each user because each password contains particular salt. Therefore, the password file is protected and it is asserted that the salt increases security.

3.9)

Password is generated with the original user password and the randomly generated salt and bother are stored in the password file using the hash function the cipher text. It might lead to resolve the problems of two users having the same salt when increasing the size of salt. If the salt is same for more users, attacker needs to do separate encryptions for each password of the user. Thus, increasing the salt to 24 or 48 bits does not protect the security of the system completely.

Review Question Chapter 4

4.1)

**Discretionary Access Control (DAC)**

* The access control is defined depends on the requestor identity and the rule of accessing authorizations.
* It allows the requestors only to do the allowed activity (Discretionary))
* The entity must have access rights to allow other entity by its own decision and enables to access some resource.

**Mandatory access control (MAC)**

* The access control is defined depends on comparing the security labels with the security clearances.
* The security label indicates whether the system resource is sensitive or critical
* The security clearance refers the system entities which are eligible to access the certain resources. (mandatory)
* The entity might not have eligibility to access the resource by its own decision and enable another entity to access some resource.

|  |  |
| --- | --- |
| **Discretionary Access Control (DAC)** | **Mandatory access control (MAC)** |
| The object owner decides which subject can access the object | The system decides which subject can access the specific data objects |
| The control access is the owner’s option | The control access is not the owner’s option of |
| Windows, Linux, MAC OS are based on DAC | Solaris and SE Linux are based on mandatory access control |
| The access control decision of the operating system is defined based on the access privileges created | The access control decision is made by the system based on the security clearance of the object |

Problem Chapter 4

4.5)

Consider a file with a protection mode 644 which is code –rw-r--r--

Code rw- is read and write access to the owner of the file

Code r-- is read access of the group of the file

Code r-- is read access of the others

The directory is having the code 730 which is code –rwx-wx---

Code rwx is read and write and execute of the directory

Code –wx is write and execute of the group

Code --- is NULL to others

Suppose the directory foo and the file test is having the same owner and group and the file test contains some text. Apart from the super user, no one can become an owner of the file test and change its contents because only the owner has write permission.

At the same time, the owner’s group has the write permission for the directory foo, so any person from the owners group can remove file test and directory foo. This also states that any person having an equivalent of rights will able to modify the file test.