**MIS 6330: IT Security**

**Prof. A. Lahiri**

**Individual Homework 4**

1. A random new challenge is sent by the host everytime the user needs to get authenticated.

This challenge is used to encrypt the hash of the password of the user along with response of the challenge.

Since, the challenge is new each time, any attacker would not be able to use replay attacks.

Also, the user is not sending the hash of the password, user will send encrypted version of the response to the challenge and hash of the password, which helps in preventing preventing an eavesdropping attacker to get hashed password directly.

Example –

User is sent a random number ***r*** by the host system and function ***f***.

The user will calculate ***f (r, h(P))***, where ***h(P)*** is the hash of the password.

Here, function ***f*** is used to encrypt the ***h(P)*** along with random number ***r*** generated by the host system.

1. For biometric systems, exact matches are not possible due to various limitations.  
   So, instead of comparing exact features, features are extracted and a score   
   is calculated based on these features during registration as well as authentication.

When user tries to authenticate, the score calculated is matched with the one stored during registration. Acceptance of user is allowed within a range of the actual value.

If the system has *lower false accept rate*, it will basically have smaller range of accepted values around the actual score.

So, the actual user may have to try more than one time, to get the score   
within accepted range and thereby, giving *lower probability of verification*   
for the user.

If the system has *higher false accept rate*, it will have bigger range of accepted   
values around the actual score.

So, the actual user will get authenticated easily and in lesser attempts.   
Thereby, giving *higher probability of verification* for the user.

However, since the range of values accepted is bigger, it might authenticate   
an impostor with a nearby score more easily.

Due to this, *probability of verification* is positively related to the *false accept rate*.

1. ***Subject*** means the entity you want to give access to. It could be owner, group or world.  
   ***Object*** means the resource on which you want to give access to the ***subject***. It could be a file, folder, etc.

***Access right*** means the type of right you want to grant to the ***object*** on the ***subject***. It could be read, write, execute, etc.

1. A table may have only ***one*** primary key while it can have as many as foreign keys as required in a RDBMS system.

**Note**: Some RDBMS system have upper limit for number of foreign keys like SQL Server 2014 has 253 as its limit. However, this number varies with systems and versions.

1. ***Role-based Access Control* (RBAC)** basically means assigning permissions   
   of access to roles and assigning roles to people instead of directly   
   assigning permissions to people (as in ACL).

The advantages of RBAC over ACL are as follows:

1. The auditing of roles as well as access given to users is easier as roles need to be checked for appropriate permissions and users need to be checked for appropriate role.
2. Adding permissions is easier as every new user needs to be assigned a pre-configured role.
3. Updating permissions is easier as each person’s individual permissions need not be checked, only the roles need to be updated. This is a huge benefit when the organization has a large number of employees.
4. Revoking permissions is easier as the user needs to be removed from their current role.
5. The benefits of creating adhoc roles with special permissions and providing a user with multiple roles are also available using RBAC.