Database Security
Access Control

By :
Dr. Rinkle Rani
Associate Professor, CSED
TIET, Patiala

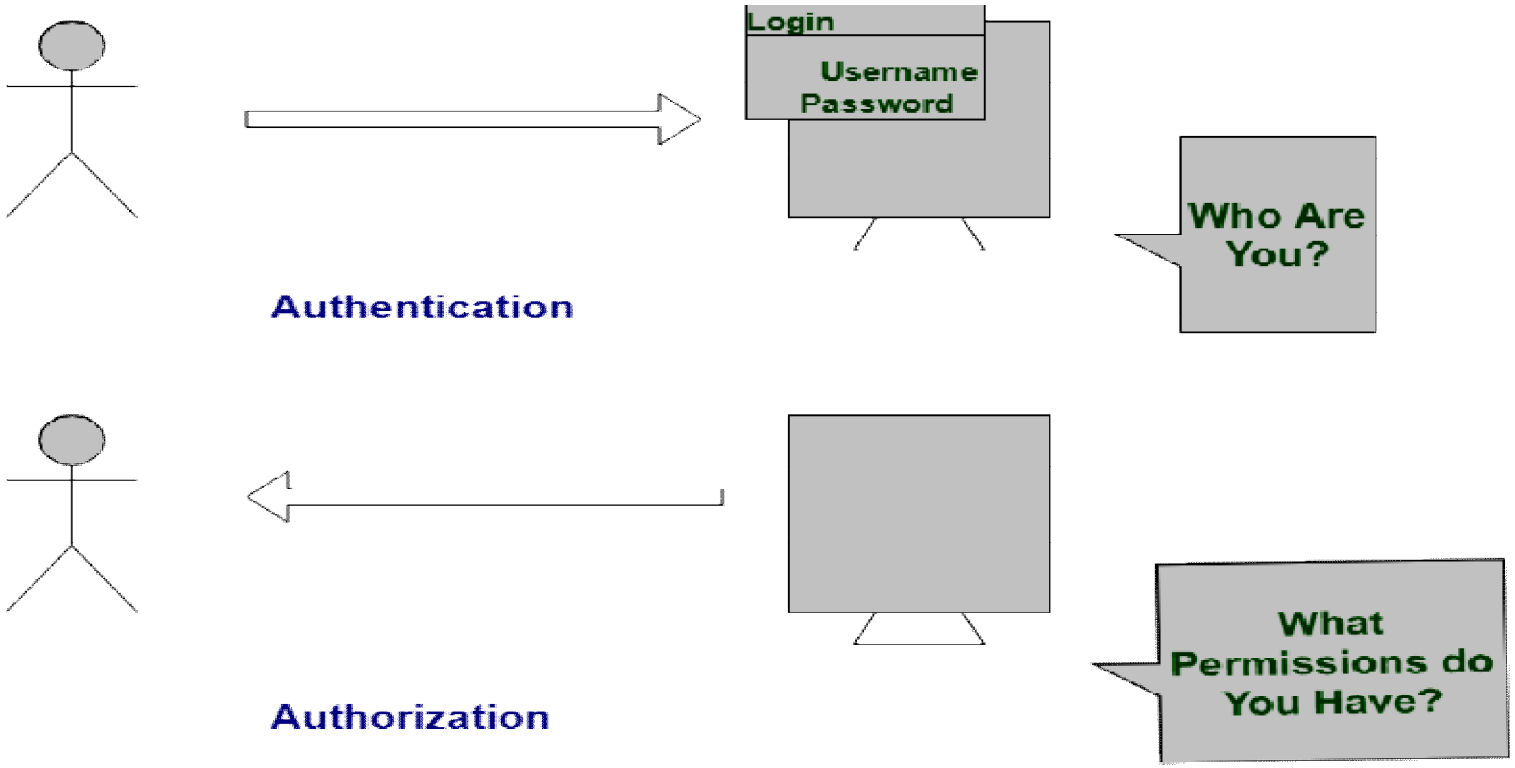
Database Security

Database Security means to keep sensitive information safe and prevent the loss of data. Security of data base is controlled by Database Administrator (DBA).

Difference between Authentication and Authorization

S.NO	Authentication	Authorization
1.	In authentication process, the identity of users are checked for providing the access to the system.	While in authorization process, person's or user's authorities are checked for accessing the resources.
2.	In authentication process, users or persons are verified.	While in this process, users or persons are validated.
3.	It is done before the authorization process.	While this process is done after the authentication process.

4.	It needs usually user's login details.	While it needs user's privilege or security levels.
5.	Authentication determines whether the person is user or not.	While it determines **What permission do user have?**



Access Control

Access control mechanisms are a necessary and crucial design element to any application's security.

In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data.

Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data.

Types of access control

Organizations must determine the appropriate access control model to adopt based on the type and sensitivity of data theyôre processing.

Access models include

1. discretionary access control (DAC) and
2. mandatory access control (MAC),
3. role based access control (RBAC) is the most common model today

What is DAC

- This model is called discretionary because the control of access is based on the discretion of the owner.
- Most operating systems such as all Windows, **Linux**, and Macintosh and most flavors of Unix are based on **DAC** models.
- DAC stands for **Discretionary Access Control**. The owner of the resource has the complete control over who can have access to a specific resource.
- The resource can be a file, directory, or any other, which can be accessed via the network.

He can grant permission to other users to access the resource.
He can also allow them to perform operations such as read, write, execute or share the resource.
Moreover, he can transfer the ownership and determine the access type of other users.

In general, DAC is an easy and flexible access control method. However, it is not very secure. As the owner of the resource has the full control, one slip from him can give full control to others.

What is MAC

- MAC stands for **Mandatory Access Control**. In this method, access is determined by the system, not by the owner. Systems that contain highly sensitive data such as government or military based systems use this access control type.
- In this control, all users (subjects) and resources should have a label assigned to them. It is a security label and specifies the level of trust.
- To access the resource, the user must have equal or higher sensitivity level than the level of the required resource.
- For example, if the user requires accessing a secret file, he should have a secret clearance or a higher clearance to access the resource.

DAC VERSUS MAC

DAC	MAC
A type of access control in which the owner of a resource restricts access to the resource based on the identity of the users	A type of access control that restricts the access to the resources based on the clearance of the subjects
Stands for Discretionary Access Control	Stands for Mandatory Access Control
Resource owner determines who can access and what privileges they have	Provides access to the users depending on the clearance level of the users. Access is determined by the system
More flexible	Less flexible
Not as secure as MAC	More secure
Easier to implement	Comparatively less easier to implement

Role Based Access Control

- In Role-Based Access Control (RBAC), access decisions are based on an individual's roles and responsibilities within the organization or user base.
- The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy.
- For instance, in a medical organization, the different roles of users may include those such as doctor, nurse, attendant, nurse, patients, etc. Obviously, these members require different levels of access in order to perform their functions

The following steps are required to implement RBAC:

1. Define the resources and services .
2. Create a mapping of roles to resources
3. Create security groups
4. Assign users to defined roles
5. Apply groups to access control lists