SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV- SECURITY ELEMENTS
Topic : Authorization and Authentication-Types, Policies and Techniques

AUTHENTICATION vs AUTHORIZATION

- **Authentication** and **authorization** are the two words used in the security world.
- They might sound similar but are completely different from each other.
- **Authentication** is used to authenticate **someone's identity**, whereas authorization is a way to **provide permission to someone to access a particular resource**.
- These are the two basic **security terms** and hence need to be understood thoroughly

What is Authentication?

- **Authentication** is the process of **identifying someone's identity** by assuring that the person is **the same as what he is claiming for**.
- It is used by both **server and client**. The server uses authentication when someone wants to access the information, and the server needs to know who is accessing the information. The client uses it when **he wants to know** that it is **the same server** that it claims to be.
- The authentication by the server is done mostly by using the **username** and **password**. Other ways of authentication by the server can also be done using **cards, retina scans, voice recognition, and fingerprints.**
- Authentication does not ensure what tasks under a process one person can do, what files he can view, read, or update. **It mostly identifies who the person or system is actually**.

Authentication Factors

As per the security levels and the type of application, there are three different types of Authentication factors:

Single-FactorAuthentication

- Single-factor authentication is the simplest way of authentication.
- It just needs a username and password to allows a user to access a system.

Two-factorAuthentication

- As per the name, it is **two-level security**; hence it needs **two-step verification to authenticate a user**.
- It does not require only a username and password but also needs the unique information that only the particular user knows, such **as first school name, a favorite destination**.
- Apart from this, it can also verify the user by sending the OTP or a unique link on the user's registered number or email address.

Multi-factorAuthentication

This is the most secure and advanced level of authorization.

- It requires two or more than two levels of security from different and independent categories.
- This type of authentication is usually used in financial organizations, banks, and law enforcement agencies.
- This ensures to eliminate any data exposer from the third party or hackers.

Authentication techniques

1. Password-based authentication

It is the **simplest way of authentication**. It requires the **password for the particular username**. If the password matches with the username and both details match the system's database, the user will be successfully authenticated.

2. Passwordless authentication

In this technique, the **user doesn't need any password**; instead, he gets an **OTP (One-time password)** or link on his registered mobile number or phone number. It can also be said OTP-based authentication.

3. 2FA/MFA

2FA/MFA or **2-factor authentication/Multi-factor** authentication is the **higher level of authentication**. It requires **additional PIN or security questions** so that it can authenticate the user.

4. Single Sign-on

Single Sign-on or **SSO** is a way to enable access to multiple applications with a **single set of credentials.** It allows the user to sign-in once, and it will automatically be signed in to all other web apps from the same centralized directory.

5. Social Authentication

Social authentication **does not require additional security**; instead, it verifies the user with the existing credentials for the available social network.

What is Authorization?

- **Authorization** is the process of **granting someone to do something**. It means it a way to check if the **user has permission to use a resource or not**.
- It defines that what **data** and **information one user can access**. It is also said as **AuthZ.**
- The authorization usually works with authentication so that the system could know who is accessing the information.
- Authorization is not always necessary to access information available over the internet. Some data available over the internet can be accessed without any authorization, such as you can read about any technology from here.

Authorization Techniques

Role-basedaccesscontrol

RBAC or Role-based access control technique is given to users as per their role or profile in the organization. It can be implemented for system-system or user-to-system.

JSONwebtoken

JSON web token or JWT is an open standard used to securely transmit the data between the parties in the form of the JSON object. The users are verified and authorized using the private/public key pair.

SAML

SAML stands for **Security Assertion Markup Language.** It is an open standard that provides authorization credentials to service providers. These credentials are exchanged through digitally signed XML documents.

Open ID Authorization

It helps the clients to verify the identity of end-users on the basis of authentication.

OAuth

OAuth is an authorization protocol, which enables the API to authenticate and access the requested resources

Authentication

Confirms users are who they say they are

Authorization

Gives users permission to access a resource

Authentication	Authorization
Authentication is the process of identifying a user to provide access to a system.	Authorization is the process of giving permission to access the resources.
In this, the user or client and server are verified.	In this, it is verified that if the user is allowed through the defined policies and rules.
It is usually performed before the authorization.	It is usually done once the user is successfully authenticated.
It requires the login details of the user, such as user name & password, etc.	It requires the user's privilege or security level.
Data is provided through the Token Ids.	Data is provided through the access tokens.
Example: Entering Login details is necessary for the employees to authenticate themselves to access the organizational emails or software.	**Example:** After employees successfully authenticate themselves, they can access and work on certain functions only as per their roles and profiles.

Any Query????

Thank you……