**DIFFERENCES BETWEEN AUTHORIZATION AND AUTHENTICATION**

Authorization and authentication are two fundamental concepts in the field of information security, often used interchangeably, but they have distinct meanings and purposes. Here are the key differences between them:

**1. Definition**

**Authentication:**

Authentication is the process of verifying the identity of a user or entity. It answers the question, "Who are you?" by checking credentials like usernames, passwords, biometrics, or other forms of identity verification.

**Authorization:**

Authorization is the process of determining what an authenticated user or entity is allowed to do. It answers the question, "What are you allowed to do?" by checking permissions and access rights.

**2. Purpose**

**Authentication:**

The purpose of authentication is to ensure that the person or system requesting access is indeed who they claim to be.

**Authorization:**

The purpose of authorization is to determine the level of access or permissions the authenticated person or system has within the application or network.

**3. Process**

**Authentication:**

Typically involves verifying a set of credentials (e.g., username and password).

May involve multi-factor authentication (MFA) using something the user knows (password), something the user has (token), and/or something the user is (biometric).

**Authorization:**

Typically involves checking the authenticated user’s permissions against an access control list (ACL), role-based access control (RBAC), or other authorization mechanisms.

Determines what resources or actions the user can access or perform.

**4. Sequence**

**Authentication:**

Always comes first. You must verify identity before you can determine access rights.

**Authorization:**

Follows authentication. Once identity is verified, permissions are checked to determine what the user can do.

**5. Examples**

**Authentication:**

Logging into a website using a username and password.

Scanning a fingerprint to unlock a device.

Using an OTP (One-Time Password) sent to a phone for accessing an account.

**Authorization:**

Checking if a logged-in user can access the admin section of a website.

Verifying if a user has permission to read, write, or delete a file.

Determining if a user can access a particular database or perform certain operations within an application.

**Example Scenario:**

**Authentication:**

A user logs into a banking application using their username and password. The system checks the provided credentials against its database to confirm the user's identity.

**Authorization:**

Once authenticated, the system checks the user's permissions to determine what features of the banking application they can access. For instance, it verifies if the user can view account balances, transfer funds, or access loan information based on their role (e.g., regular user vs. bank manager).

**Summary:**

Authentication verifies who you are.

Authorization determines what you are allowed to do.

Both are critical for maintaining security in systems and applications, ensuring that users are properly identified and only have access to resources and actions they are permitted to use.