Difference between Authorization and Authentication

Feature	Authentication	Authorization
Definition	Verifying the identity of a user	Granting or denying user access to resources
Purpose	To confirm who the user is	To determine what the user is allowed to do
Process	Involves checking credentials (e.g., username and password)	Involves checking permissions and access levels
Timing	Happens before authorization	Happens after authentication
Data Used	User credentials (username, password, biometrics)	User roles, permissions, and access controls
Outcome	User is identified	User is granted or denied access to resources
Scope	Focuses on user identity	Focuses on user privileges and permissions
Examples	Logging into a system	Accessing specific files, functions, or data within the system
Protocols	Protocols like OAuth, OpenID Connect, SAML for identity verification	Protocols like OAuth, RBAC (Role-Based Access Control), ACL (Access Control List) for permission management
Implementation	Requires user to provide valid credentials	Requires a system to have predefined permissions and access rules
User Interaction	Direct interaction required (e.g., entering a password)	Typically indirect, based on predefined access levels
Security Focus	Ensures the person is who they claim to be	Ensures authenticated users can only access what they're permitted to
Common Mistakes	Weak passwords, credential theft	Incorrectly configured permissions, excessive privileges