

Authentication is the process of verifying identity, who are you that is trying to access a system. While authorization is the process that happens after authentication has passed. Authorization refers to what you can do, based on your role/permission. A type of authorization is Role Based Access Control (RBAC) - this is a mechanism that assigns roles and these roles come with predefined permissions. For example, someone given the role "Editor" can edit, view, and create.

Another type of authorization is Access control Lists (ACLs): permissions are defined for each user based on a specific resource. The system maintains a list that provides what users can do when it comes to resources allocated to them. For example: User A can read this certain file, while user B can write to it. And maybe the others can execute it.

The Principle of Least Privilege. When it comes to the principle of least privilege. It gives users minimum permissions necessary to complete their task and nothing more. This type of authorization is suitable for situations where you would hire a temporary user to do a task but they would not need entire access to your system, but rather maybe a directory for completing such task.