Authentication vs. Authorization

Authentication and authorization are the core principles when it comes to security. Authentication verifies the user's identity ("Who are you?") using methods like username & password pairing or biometrics. While authorization, determines the "What are you allowed to do once logged in" by managing the resource access for authenticated users, by assigning roles. With authorization (Role-based access control (RBAC) permissions are assigned through roles. For example, "Admin" might have the ability to access all features of the system, while "editor" can view and modify content only. (A common example of this is google drive's share option). For access control list (ACLs), this specifies permissions per resource and user. An ACL for a file might allow John to read/write and Mark (another user on the same machine) to just be able to read it only. Which offers a fine-grained control but is risky based on the complexity of said system. Principle of Least Privilege, minimizes the user's permissions to a standard level, which minimizes the damage from breaches.