Authentication is the verification of a user's identity ensuring they are who they claim to be. Authorization determines what resources a user can access and what actions they are allowed to do. Authorization usually comes after authentication and the user's permissions are granted by the owner of the system. Role-based access controls refer to assigning users with distinct roles that each come with different permissions. Users are typically granted roles at user creation. After being logged-in whenever the user tries to access a resource their role and its permissions is checked. Access control list assigns individual permissions to users and when a user tries to access a file or resource checks if the permission required by the file matches the permission in their permission list. The principle of least privilege states that a user should have as little access needed to accomplish their tasks. An example of this would be that a marketing manager should have access to the necessary data in order to fulfill their tasks but shouldn't have access to the software development environment.