Authorization is the process of controlling who has access to certain resources. Authentication however, verifies user identity to ensure that they are who they claim to be. After authentication happens and a user's identity is confirmed authorization goes a step further and gives a user access to certain privileges. For example after a user inserts their pin and goes to edit a file in a system they are either allowed or not allowed to perform that action. Types of authorization are Role-based access control (RBAC) which determines a user's access permissions based on their roles, Attribute-based access control (ABAC) which use the attributes of users, objects and actions like a user's name, a resource's type and the time of day to determine what all is accessible to them. An important concept in authorization is the Principle of Least Privilege which ensures that users have the least amount of privileges possible while being able to perform their tasks. This concept helps to protect a system against malicious or accidental wrongdoings. Both authentication and authorization are needed to have a safe system that protects sensitive information and network resources.