Jael Johnson
CMPS-2131

Authorization controls what users can do or access after a user is authenticated by the system. Authentication is simply identifying a user (logging in with a username and a password), while authorization is defining what is permitted to a user after their identity is authenticated.

Role-Based Access Control (RBAC) is a common authorization method. Users are assigned roles (admin or user), and each role has predefined permissions. For example, system admins may have unrestricted access while regular users may have system access, but it is limited in some way. This helps simplified permission management by access rights are grouped.

Access Control Lists (ACLs) are another mechanisms. These are lists attached to resources that specify what actions users or groups of users can perform. For example, one user may have read/write access to a file while another user can only read it, and this permission is defined in the files ACL.

The Principle of Least Privilege (PoLP) is another important core security principle. It provides users only the access and permissions they need to perform their tasks. This helps minimize risks associated with system misuse and mistakes.

In summation, authentication is identifying a user and authorization is defining what a user can do. Effective system access control hinges on the use of PoLP, ACLs, and RBAC to keep systems secure.