Authorization Write-Up

Authorization is the mechanism used to control what an authenticated user can do within a system. While authentication states "Who are you?", authorization states "What can you do?". In reality, they complement each other with secure systems: authentication checks identity, and authorization enforces boundaries.

One of the most popular models of authorization is Role-Based Access Control (RBAC), where permissions are organized into roles like "admin," "editor," or "viewer." The user's ability is distinguished by their respective role, which is simpler to manage if there are numerous users with similar tasks. Another method is Access Control Lists (ACLs), where individual permissions are directly applied to users or resources. ACLs are highly specific in control but are invasive in large environments.

The other rule that can be applied to both ACLs and RBAC is that of the least privilege. This is a matter of granting users only what they absolutely need for their work. For example, an editor will have to create and change documents but not system controls. Least privilege reduces the risk of accidental or erroneous use because fewer operations are available to any individual account.

In short, authentication is aided by authorization, which limits even authorized users to go beyond their granted access.