Umar Amjad
Software Developer

Authentication vs Authorization

Authentication

* Authentication verifies the identity of a user or system.

* Techniques include passwords, biometric authentication, smart cards, and two-factor authentication.

Authorization

* Authorization determines what resources or actions a user or system is allowed to access.

* Techniques include access control lists, role-based access control, and attribute-based access control.

Difference between Authentication and Authorization

* Authentication confirms identity, while authorization determines access.

* Authentication occurs before authorization.

* Techniques for authentication include passwords and biometric authentication, while techniques for authorization include access control lists and role-based access control.

Popular Techniques Of Authentication

Passwords: Users provide a secret password that is matched against a stored value to verify their identity.

Biometric authentication: Users provide a biological characteristic, such as a fingerprint or facial recognition, which is verified against a stored value.

Smart cards: Users provide a physical card containing a chip or magnetic stripe that stores their identity information.

Two-factor authentication: Users provide two forms of identification, such as a password and a code sent to their phone, to verify their identity.

Single sign-on: Users authenticate once with a central authentication system and are then granted access to multiple applications or systems without needing to re-authenticate.

OAuth: Users authenticate with a third-party provider, such as Google or Facebook, which then grants access to applications or systems that support OAuth authentication.

Popular Techniques Of Authorization

Access control lists (ACLs): A list of permissions that specifies which users or groups have access to which resources.

Role-based access control (RBAC): Users are assigned to roles that have specific permissions, and access to resources is granted based on the user's assigned role.

Attribute-based access control (ABAC): Access to resources is determined based on a set of attributes associated with the user, such as their job title or department.

Rule-based access control (RBAC): Access to resources is determined based on a set of rules that specify which users or groups have access based on various conditions, such as time of day or location.

Mandatory access control (MAC): Access to resources is determined by a set of rules defined by a central authority, such as a system administrator or security policy.

Discretionary access control (DAC): Access to resources is determined by the owner of the resource, who can grant or deny access to other users.

Thanks...

Umar Amjad
Software Developer