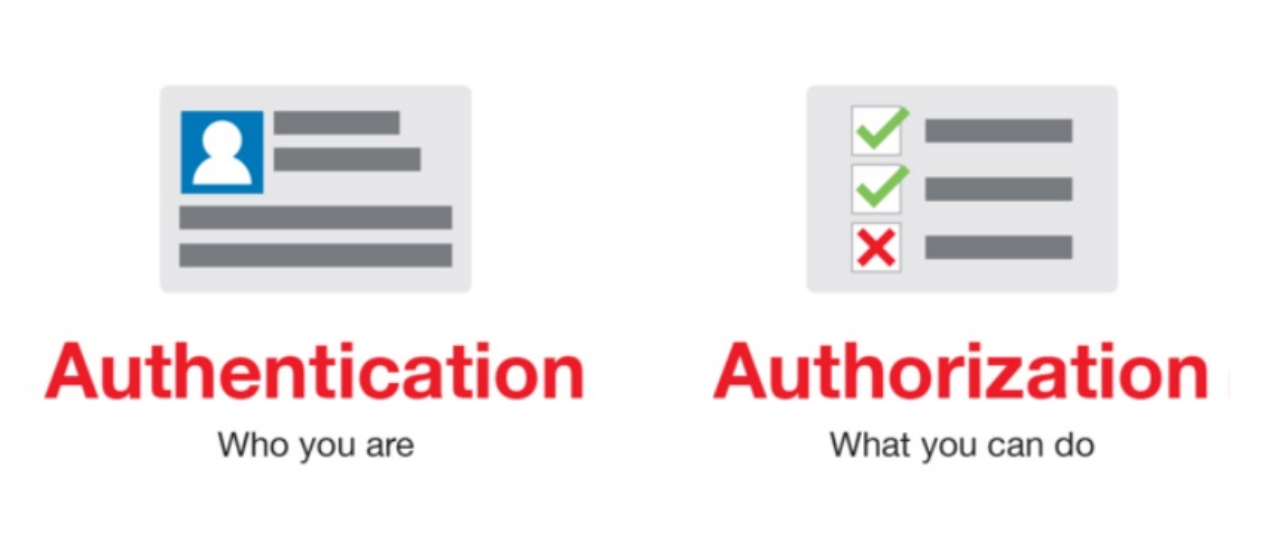
Authentication and Authorization



인증 (Authentication)

인증(Authentication)은 사용자가 자신이 주장하는 신원이 실제로 그 사용자와 일치하는지를 확인하는 프로세스입니다. 인증은 시스템에 접근하려는 사용자의 신원을 확인하여, 시스템 자원에 대한 권한 부여를 결정하는 데 사용됩니다.

다양한 인증 방법과 기술이 있지만, 가장 일반적인 방법은 사용자 이름과 비밀번호를 사용한 인증입니다. 사용자 이름과 비밀번호를 입력하면 시스템은 해당 정보가 정확한지 확인합니다. 이 방법은 간단하지만, 비밀번호가 노출되면 보안 위험에 노출될 수 있습니다.

OAuth는 인증 및 권한 부여를 위한 업계 표준 프로토콜 중 하나입니다. OAuth는 서드파티 서비스에서 사용자의 인증 정보를 공유하여 사용자의 권한 부여를 처리합니다. 사용자는 자신의 인증 정보를 직접 제공하지 않고, 서드파티 서비스를 통해 권한 부여를 받을 수 있습니다.

JWT(Json Web Token)는 인증을 위한 다른 방법입니다. JWT는 JSON 형식으로 인코딩된 토큰을 사용하여 인증을 수행합니다. JWT에는 사용자 ID 및 사용자 권한과 같은 정보가 포함되어 있습니다. 서버에서 JWT를 생성하고 클라이언트에게 전달되면, 클라이언트는 JWT를 사용하여 인증을 수행할 수 있습니다.

인가 (Authorization)

인가(Authorization)는 인증된 사용자가 특정 자원에 대한 접근 권한이 있는지 여부를 결정하는 과정입니다. 즉, 인증된 사용자에 대해 "어떤 것을 할 수 있는지"를 정하는 것입니다. 인가를 통해 사용자는 자신이 필요한 것만 볼 수 있고, 다른 사용자들의 데이터를 보거나 변경하는 것을 방지할 수 있습니다.

인가를 위해 사용되는 방법과 기술에는 여러 가지가 있습니다. 그 중에서도 가장 일반적인 것은 역할 기반 접근 제어(Role-Based Access Control, RBAC)입니다. RBAC는 사용자의 역할(role)에 따라 권한을 부여하는 방식입니다. 예를 들어, "관리자"라는 역할은 모든 자원에 대한 읽기, 쓰기 및 삭제 권한을 가지고 있으며, "사용자"라는 역할은 자신의 정보에 대한 읽기 권한만 가지고 있습니다. RBAC를 사용하면 권한을 관리하는 것이 쉽고, 보안성도 높일 수 있습니다.

또 다른 인가 방법은 액세스 제어 목록(Access Control List, ACL)입니다. ACL은 각 자원에 대해 허용되는 사용자 또는 그룹을 명시하는 방식입니다. 예를 들어, 파일 서버의 특정 파일에 대한 접근을 허용할 때, 특정 사용자 또는 그룹에 대한 권한을 명시합니다.

OAuth와 JWT는 인가를 위한 다른 방법입니다. OAuth는 사용자가 자신의 데이터를 다른 웹 사이트 또는 애플리케이션과 공유할 수 있도록 하는 프로토콜입니다. OAuth는 사용자의 권한을 관리하기 위해 인가 코드(authorization code)와 엑세스 토큰(access token)을 사용합니다.

JWT는 인증과 인가를 모두 수행할 수 있는 토큰 기반의 인증 방법입니다. JWT는 토큰 자체에 사용자 정보와 권한 정보를 포함시키기 때문에, 서버에서 별도의 세션 정보를 저장하거나 데이터베이스를 조회할 필요가 없습니다. JWT는 자체적으로 인증을 수행할 수 있기 때문에, OAuth와 함께 사용될 수 있습니다.

최신 인증과 인가 기술과 트렌드

FIDO2

FIDO2(Fast Identity Online 2)는 패스워드 대신 바이오메트릭 센서, 보안 키, PIN 등을 사용하여 강력한 인증을 제공하는 개념입니다. FIDO2는 웹 브라우저와 모바일 디바이스에서 작동하며, 네이티브 앱에서도 사용할 수 있습니다. FIDO2는 사용자 경험을 개선하고 동시에 보안 수준을 높이는 데 큰 역할을 합니다.

OAuth 2.0

OAuth 2.0은 애플리케이션 간 인증과 인가를 위한 개방형 표준 프로토콜입니다. OAuth 2.0을 사용하면 사용자가 소셜 미디어 앱이나 기타 애플리케이션에서 제공하는 서비스에 대해 인증 및 인가할 수 있습니다. OAuth 2.0은 새로운 기능과 보안 업데이트가 지속적으로 추가되고 있습니다.

OpenID Connect

OpenID Connect는 OAuth 2.0 프로토콜을 기반으로 하며, 사용자의 ID와 인증을 위한 표준화된 방법을 제공하는 개방형 표준 프로토콜입니다. OpenID Connect는 웹과 모바일 애플리케이션에서 강력한 인증을 제공하며, 일반적으로 OAuth 2.0과 함께 사용됩니다.

SAML

SAML(Security Assertion Markup Language)은 인증 및 인가 정보를 XML 형식으로 교환하는 프로토콜입니다. SAML은 단일 로그인(Single Sign-On, SSO) 시스템과 함께 사용됩니다. SAML은 기존 시스템과 통합하기 위한 목적으로 많이 사용되며, 기존 인프라와의 호환성이 높은 것이 장점입니다.

블록체인 기반 인증

블록체인 기반 인증은 블록체인 기술을 이용하여 인증을 수행하는 방식입니다. 블록체인은 탈중앙화된 분산 네트워크를 구성하며, 블록체인에 저장된 정보는 변경이 불가능하고 안전하게 보호됩니다. 블록체인을 이용한 인증은 중앙 기관 없이 개인이 직접 인증을 수행할 수 있어 보안성이 높고, 탈중앙화된 특성 때문에 위조나 변조가 어렵습니다. 블록체인을 이용한 인증 기술은 현재 블록체인 기반 신원 확인(ID) 및 인증 기술이 주로 사용되고 있으며, 이를 토대로 보다 안전하고 신뢰성 있는 인증 및 인가 기술의 발전이 기대됩니다.

결론

항목	Authentication	Authorization
정의	사용자의 신원 확인	액세스 권한 확인
목적	자신이 누구인지 확인하도록 사용자를 확인	사용자에게 특정 리소스에 대한 액세스 권한이 있는지 확인
방법	사용자 이름, 망막 스캔, 얼굴 인식 등과 같은 요소를 통해 사용자를 식별	미리 지정된 규칙을 통해 리소스에 엑세스 할 수 있는 사용자의 권한을 확인
순서	Authorization전에 수행	Authentication 후에 수행