**Discussion 6.1 – OAuth and OpenID Connect**

Patrick Cuauro

Bellevue University

WEB 420-307O RESTFul APIs

Professor Krasso

June 27, 2023

OAuth 2.0 and OpenID Connect are two open standards that allow third-party applications to access protected resources, such as user data, on behalf of a user.

OAuth 2.0 is a framework for authorization. It defines a set of flows that allow an application to request access to protected resources on behalf of a user. The OAuth 2.0 flow typically involves the following steps:

1. The user authorizes the application to access their resources.
2. The application requests an access token from the authorization server.
3. The authorization server grants the access token to the application.
4. The application uses the access token to access the protected resources.

OpenID Connect is an authentication layer that builds on top of OAuth 2.0. It adds an ID token to the OAuth 2.0 flow, which contains information about the user who authorized the application. The ID token can be used by the application to verify the user's identity and to obtain additional information about the user, such as their name, email address, and profile picture.

The main difference between OAuth 2.0 and OpenID Connect is that OAuth 2.0 is only concerned with authorization, while OpenID Connect is also concerned with authentication. OpenID Connect is a more comprehensive solution for applications that need to verify the identity of their users.

Here is a table that summarizes the key differences between OAuth 2.0 and OpenID Connect:

|  |  |  |
| --- | --- | --- |
| Feature | OAuth 2.0 | OpenID Connect |
| Purpose | Authorization | Authorization and authentication |
| ID token | Not Required | Required |
| Information about the user | Not included | Included in the ID token |
| Use cases | Accessing protected resources | Verifying the identity of users and obtaining additional information about them |

OAuth 2.0 and OpenID Connect are both widely used standards. OAuth 2.0 is the more popular of the two, but OpenID Connect is gaining in popularity because it provides a more comprehensive solution for applications that need to verify the identity of their users.

Here are some examples of applications that use OAuth 2.0 and OpenID Connect:

* Social media apps such as Facebook, Twitter, and LinkedIn use OAuth 2.0 to allow users to log in to their apps with their social media credentials.
* Webmail apps such as Gmail and Outlook use OAuth 2.0 to allow users to access their email accounts from third-party applications.
* Single sign-on (SSO) solutions use OpenID Connect to allow users to sign in to multiple applications with a single set of credentials.

Sources:

<https://developer.okta.com/docs/concepts/oauth-openid/>