William Austin

06/28/2023

Discussion 6.1 - OAuth and OpenID Connect

OAuth and OpenID Connect (OIDC) are two authentication protocols used for web applications. They both allow users to grant access from one resource on the internet to another resource. The main difference is the amount of access granted. (Barak, 2022)

OAuth is mainly used to allow users to grant limited access to their resources on one service to another service without sharing their credentials. The best way to explain this is through an example. Let’s say you create an Instagram account, and it asks “Can we have access to your email contacts, so we can let them all know you’re on Instagram”. If you (the user) allow this, Instagram (the client) can access your contact list on Gmail (the resource provider). That’s all they can do. They can’t see your emails, or know anything about your login information or really understand any more about you (the user). This is done more specifically through something called the OAuth flow, which involves a series of Access tokens and Client Secrets that would take much too long to detail in this post.

OpenID Connect is a layer built on top of OAuth. You must have OAuth to have OIDC. It enables a client to authenticate the users through ID tokens. It grants the client much more access to information about the User and, possibly, much more data from the Resource Provider. If OAuth is a key to a certain door, OIDC is an ID badge, that not only allows access to that door, but also shares with the client all sorts of information about the user. OIDC focuses less on authorization to access a resource and more on Identity Management. You’ve seen a site ask, would you like to create an account using Facebook. That is a form of OIDC. Facebook knowns your identity, and can thus create the account on "IFeelLikeA[BeautifulMe.com](http://BeautifulMe.com)". Facebook uses your ID token to tell the website that you are who you say you are, and that’s good enough for

"IFeelLikeA[BeautifulMe.com](http://BeautifulMe.com)". (OktaDev, 2019).

OIDC is also in something like Google. Where one sign on allows you access to multiple applications. This is something known as single sign-on or SSO. Hopefully, adding a level of convenience without compromising security.

OIDC and OAuth are both used in authentication, but the level of authentication and what can be done with that authentication is where they are separate. OIDC is built on top of the framework of OAuth and allows for SSO and Identity management. OAuth is more about data access and authorization.

**Sources**

Barak, S. (2022, January 14). *OAuth 2.0 and openid connect for dummies*. Medium. https://medium.com/everything-full-stack/oauth-2-0-and-openid-connect-for-dummies-6fa6e995d6d5

Lauret, A., & Lane, K. (2019). *The design of web apis*. Manning.

OktaDev. (2019, November 5). *An Illustrated Guide to oauth and OpenID connect*. YouTube. https://www.youtube.com/watch?v=t18YB3xDfXI