Post by Pearce Begley
Peer response

Open authentication, as saidabove, is widely used. However, it can be susceptible to brute force hacking.Brute force hacking is when there is an attack on a network via waiting andlearning specific request parameters. Once the hacker understands enough of therequests, they can create something called a packet. A packet of data is thencaptured via a packet sniffer and allows the brute force attack to start.Tokens can also be created to help reduce the chance of a brute force attackbut are not perfect. Tokens are a portable device that authenticates identityelectronically. An example is a USB token. Tokens can be hacked, often due tohuman error. Tokens are a cheap form of cyber security and often not difficultfor users to use. It is also important to distinguish the difference betweenauthentication and authorization. Authentication is making sure the identity iscorrect. Authorization is not confirming users' identity but determining whichareas users can access and what they are allowed to do with the resources. Theabove post discussed federation protocol. A Federated identity is a user whocan access lots of different websites with only one login, which is used withOAuth 2.0. It is also important to bringup botnets. Botnet maintains a user-friendly experience for online users byconnecting computers and websites when doing receptive tasks such as a relaychat. They are legal to use but sometimes defective botnets can gain accessthrough coding and cause security issues. Often masking botnets can assist inDDoS attacks. Spoofing is also an important issue to discuss. There aredifferent types of spoofing, IP addresses, address resolution, domain namesystem, and email spoofing. Spoofing can be used for legitimate reasons. Forexample, IP spoofing can be used to test server capacity and testingsecurity.

References: Clarke, I; Friedman, A. (2021).OAUTH abuse: think solarwinds/ solarigate campaign with a focus on cloudapplications.
Available: https://www.proofpoint.com/us/blog/cloud-security/oauth-abuse-think-solarwindssolorigate-campaign-focus-cloud-applications. Lastaccessed 11th April 2022. Copeland, T. (2019). How tocreate a security token and run an STO.
Available: https://decrypt.co/5882/create-security-token-run-offering. Lastaccessed 11th April 2022. Hack_EDU. (2021). CommonFederated Identity Protocols: OpenID Connect vs OAuth vs SAML 2.Available: https://www.hackedu.com/blog/analysis-of-common-federated-identity-protocols-openid-connect-vs-oauth-2.0-vs-saml-2.0. Lastaccessed 11th April 2022. Kiani, K. (2011). Four Attackson OAuth - How to Secure Your OAuth Implementation. Available: https://www.sans.org/blog/four-attacks-on-oauth-how-to-secure-your-oauth-implementation/. Lastaccessed 11th April 2022. Majaski, C. (2020). SecurityToken Definition. Available: https://www.investopedia.com/terms/s/security-token.asp. Lastaccessed 11th April 2022. O'Donnell, A. (2021). What ArePacket Sniffers and How Do They Work?. Available: https://www.lifewire.com/what-is-a-packet-sniffer-2487312. Lastaccessed 11th April 2022. okta. (2022). FederatedIdentity.
Available: https://developer.okta.com/books/api-security/authn/federated/. Lastaccessed 11th April 2022.