Explain how Oauth works and how it relates to computer security. Justify your rationale.

OAuth (Open Authorization) is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites without sharing their credentials. OAuth works by enabling users to grant third-party access to their resources stored on a given server without sharing their credentials. It is commonly used as a method for users to log into third-party websites using their Google, Facebook, or Twitter accounts, without sharing their login credentials with the third-party site.

Here's how OAuth works:

The user grants permission to a third-party application to access their resources on a server on their behalf. The third-party application requests an access token from the server, presenting the user's authorization grant. If the user's credentials are valid and the authorization grant is accepted, the server issues an access token to the third-party application. The third-party application uses the access token to access the user's resources on the server.

OAuth enhances computer security by reducing the exposure of user credentials, empowering users to control data access, providing a standardized approach to authorization, and enabling centralized and secure access control. By leveraging OAuth, organizations and users can benefit from improved security practices when granting third-party access to user resources.

References:

Sobers, R. (2012, April 5). What is OAuth? Definition and How it Works. Www.varonis.com. https://www.varonis.com/blog/what-is-oauth

What is OAuth 2.0 and what does it do for you? (n.d.). Auth0. https://auth0.com/intro-to-iam/what-is-oauth-2