OAUTH 2.0:
SECURING MODERN APPLICATIONS

In this PDF:

- What is OAuth 2.0 and why is it important?
- What are the key roles in the OAuth 2.0?
- How does the OAuth 2.0 flow work?
- What are the different types of OAuth 2.0 grant types?
- What role do tokens play in OAuth 2.0?
- What are the benefits of OAuth 2.0 and best practices for implementation?

Mahyah Binti Idris

OAuth 2.0 is the industry-standard protocol for authorization that enables applications to obtain limited access to user accounts.

It provides a secure way for users to grant access to their resources without sharing their credentials.

Key points:

- Enables secure third-party access to resources
- Separates authentication from authorization
- Supports various client types and devices
- Eliminates the need to share passwords

Mahyah Binti Idris

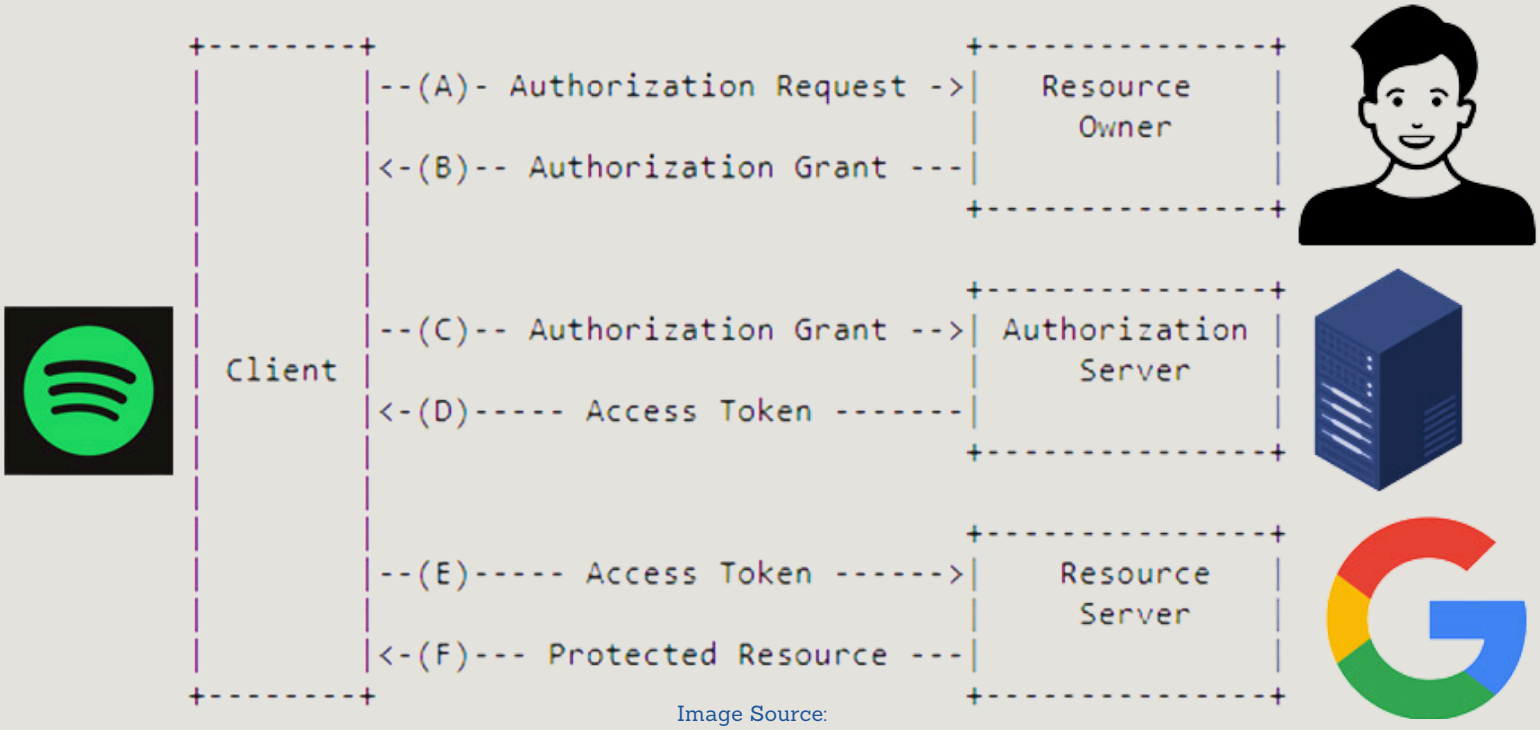

Image Source:
http://makeseleniumeasy.com/2023/02/08/2-oauth-2-0-flow-authorization-grants-and-their-types/

OAuth 2.0 defines four key roles:

Resource Owner:
The user granting access to their data

Client:
The application requesting access to the user's data

Authorization Server:
Authenticates the user and issues access tokens

Resource Server:
Hosts the protected user data

Mahyah Binti Idris

OAuth 2.0 flow overview:

- Client requests authorization from Resource Owner
- Resource Owner grants authorization
- Client requests access token from Authorization Server
- Authorization Server issues access token to Client
- Client requests resource from Resource Server using access token
- Resource Server validates token and serves resource

Mahyah Binti Idris

AUTHORIZATION GRANT TYPES

Authorization Code:
Secure flow for web apps. Server exchanges code for access token, keeping credentials confidential.

Implicit:
Simplified flow for single-page apps. Token returned directly to browser, suitable for public clients.

Resource Owner Password Credentials:
Direct username/password exchange. Used for highly-trusted, first-party applications only.

Client Credentials:
Machine-to-machine authentication. Allows apps to access their own resources, not user-specific data.

Each grant type is suited for different scenarios and security requirements.

Mahyah Binti Idris

TOKENS IN OAUTH 2.0

OAUTH 2.0 USES TWO TYPES OF TOKENS:

Access Tokens:

Short-lived tokens used to access protected resources

Refresh Tokens:

Long-lived tokens used to obtain new access tokens

Mahyah Binti Idris

BENEFITS & BEST PRACTICIES

Benefits:

- Enhanced security
- Improved user experience
- Scalability and flexibility

Best Practices:

- Use HTTPS for all OAuth 2.0 interactions
- Use state parameters to prevent CSRF attacks
- Securely store client secrets and tokens
- Use official OAuth libraries when building your app

Mahyah Binti Idris

Thank You

FOR READING!

Share