Desenvolvimento de Componentes Distribuídos - API

Lidiane Gomes Batista Slisinski

1. Para que serve e para que foi criado o protocolo OAuth?

O OAuth é um recurso utilizado para autenticação de usuários utilizando o cadastro de outra plataforma (Google, Facebook, Twitter), onde a aplicação envia para esta plataforma os acessos e ela validará e enviará uma autorização ou rejeição para o acesso do usuário. Deixando exclusivamente os dados do usuário na plataforma. Ele foi criado para garantir a segurança na comunicação entre aplicações e a proteção aos dados do usuário.

1. Descreva o fluxo do protocolo OAuth na versão 2.0:

Ele foi construído em cima de quatro papéis(Roles): Proprietário do Recurso (Resource Owner), Cliente (Client), Servidor de Recurso (Resource Server) e o Servidor de Autorização (Authorization Server).

- O Resource Owner é a pessoa/entidade que concede o acesso aos seus dados.

- Client é a aplicação que interage com o Resource Owner no caso da aplicação web, seria a aplicação no browser.

- Resource Server – a API que está exposta na internet e precisa de proteção dos dados. Pra conseguir acesso ao seu conteúdo é necessário um token emitido pelo Authorization Server.

- Authorization Server – responsável por autenticar o usuário e emitir os tokens de acesso. É ele quem possui as informações do Resource Owner, o usuário. Autentica e interage com o usuário após a identificação do Client.

Fluxo utilizado durante processo de autorização:

1ª etapa - A aplicação solicita autorização para acessar os recursos do usuário no servidor.

2ª etapa - Se o usuário autorizar a solicitação a aplicação recebe uma concessão de autorização.

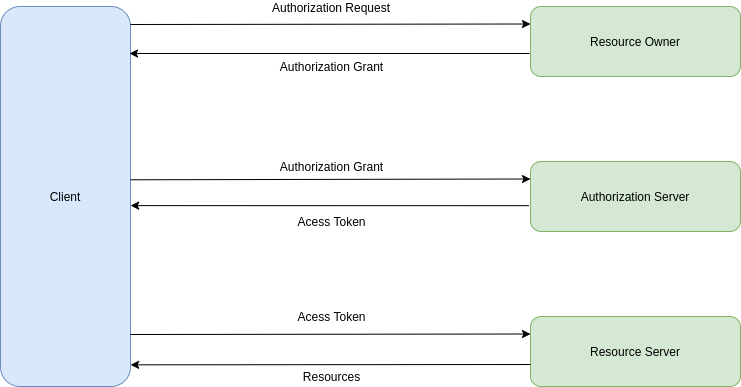
3ª etapa - A aplicação solicita um token de acesso ao servidor de autorização (API) através da autenticação da própria identidade e da concessão de autorização.

4ª etapa - Se a identidade da aplicação está autenticada e a concessão de autorização for válida, o servidor de autorização emite um token de acesso para aplicação.

A autorização nesta etapa já está completa e o cliente já terá um token de acesso para gerenciar.

5ª etapa - Quando a aplicação precisar solicitar um recurso ao servidor de recursos, basta apresentar o token de autenticação.

6ª etapa - Se o token de acesso for válido, o servidor de recursos fornece o recurso para a aplicação.



https://medium.com/equals-lab/protocolo-de-autoriza%C3%A7%C3%A3o-oauth-2-0-561542a39f2d

1. Descreva como este serviço, se mal utilizado, pode trazer problemas de segurança para uma empresa.

A segurança da empresa será ameaçada se tivermos problema com o token. Por exemplo: se o token recebido for armazenado de forma indevida, ou seja, suscetível a roubo desta informação, ficará vulnerável ao acesso e uso indevido de informações secretas da empresa.

1. Cite pelo menos 10 serviços de grandes empresas provedoras de autorização que utilizam este protocolo.

|  |  |  |  |
| --- | --- | --- | --- |
| Facebook | Google | GitHub | Twitter |
| Microsoft | Youtube | IBM | Amazon |
| Twitch | Yahoo | TV Globo | Alibaba |