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

O protocolo OAuth 2.0 foi criado com a intencão de limitar o acesso de aplicativos externos dentro do protocolo HTTP, onde é criado um layer de autorização(authorization server), que serve para separar a aplicação(client) do usuário(resource owner), onde é gerado um token de acesso, que, após a verificação dos dados no servidor(resource server), concede o acesso à aplicação.

2. Descreva o fluxo do protocolo OAuth na versão 2.0"

Quais os agentes envolvidos ?

Resource owner – Geralmente é o usuário que da acesso aos dados privados;

Resource server – É o servidor que guarda e autentica os dados do usuário, assim sendo a entidade que da acessou ou não ao token de autenticação;

Client – É a aplicação que interage com o usuário (não se limita somente a aplicações web);

Authorization server – O servidor que garante, ou não, os access tokens aos usuários, após a comunicação com o resource server.

Qual o fluxo de informação entre estes agentes ?

---------- | Etapas

Client -------Solicita autorização----------→ Resource owner | 1.

Client < ----- Concede autorização ---------- Resource owner | 2.

Client ----- Concessão da autorização-------→ Authorization Server | 3.

Client <----------Token de acesso ---------- Authorization Server | 4.

Client ---------- Token de acesso ----------→ Resource server | 5.

Client < ------- Recurso Protegido ------- Resource server | 6.

(1.) Na primeira etapa, o lado da aplicação solicita uma autorização do usuário para acesso aos recursos privados (sendo de forma direta, apenas pedindo as credenciais, ou de forma indireta, usando o servidor de autorização como mediador). **(2.)** Após a concessão do usuário, geralmente representada por alguma credencial, **(3.)** o client solicita um token de acesso ao servidor de autorização, enviando a concessão do usuário. **(4.)** Nessa etapa, o servidor de autorização valida as credenciais e, caso corretas, emite um token de acesso à aplicação, que em seguida, **(5.)** manda o token ao resource server, **(6.)** que verifica o token e, caso valido, retorna ao client o recurso solicitado.

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

O serviço Oauth pode trazer problemas quando utilizado para autenticação e não para autorização, assim, não utilizndo o serviço de maneira certa. O protocolo usa os tokens de acesso para autenticação de um usuário, porém, esse token, quando usado para autorização, não serve para função, já que um token de acesso não representa um usuário necessáriamente, podendo ser uma maquina usando as credenciais do usuário, que nesse caso, permitiria qualquer um, com as credenciais da pessoa em questão, ter um token de acesso à conta dela.

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

Google

Twitter

Facebook

Microsoft

Github

Oracle

Discord

Amazon

Yahoo!

Spotify