SAFE AND EASY SURFING IN THE INTERNET

It would be wondering for us how the websites/web portals provide us with the services that is required.If it is keenly noted we would know that we provide our credentials only once during the process but we are provided with the services continuously without being asked for our credentials many times.It is based on the protocols and frameworks used in the web.One such protocol is the Oauth.

OAuth:

Oauth is an open Authorizaion Protocol which is used to access the resources of the resource owner in the server.

Oauth will be easy to implement and more secure since it uses the SSL(Secure Socket Layer) to save the user tokens and it is more flexible.

Oauth is used when a third party is involved in the process (i.e)when the resources sharing should be authorized by the resource owner to the server.

The client app,resource owner and then the resource and authorization server are the three parties invloved.

Client requests resource from the resource server for which authorization is required which is carried out in Oauth.

Tokens:

Tokens are the alternates for the credentials.Tokens will be generated once the client is authenticated or authorized.

Tokens are used as the verification parameter as it is a part of the url being used.

Oauth Workflow:

Implicit Flow:

In this method the access token is directly provided to the client by the authorization server once it is verified with he resource owner.

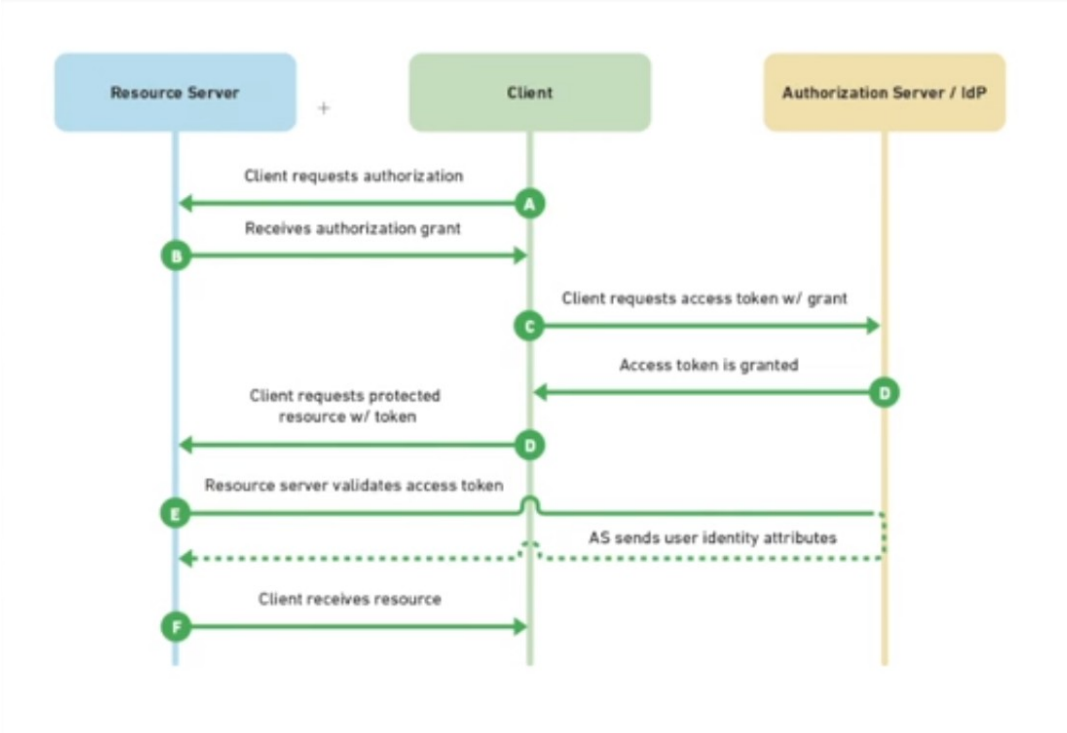
This is not so secure and used in Javascript apps

Authorization Code Flow:

Here the Authentication token is given first and then the Access token was given when the request was made again by the client to the Authorization server with the Authentication token.

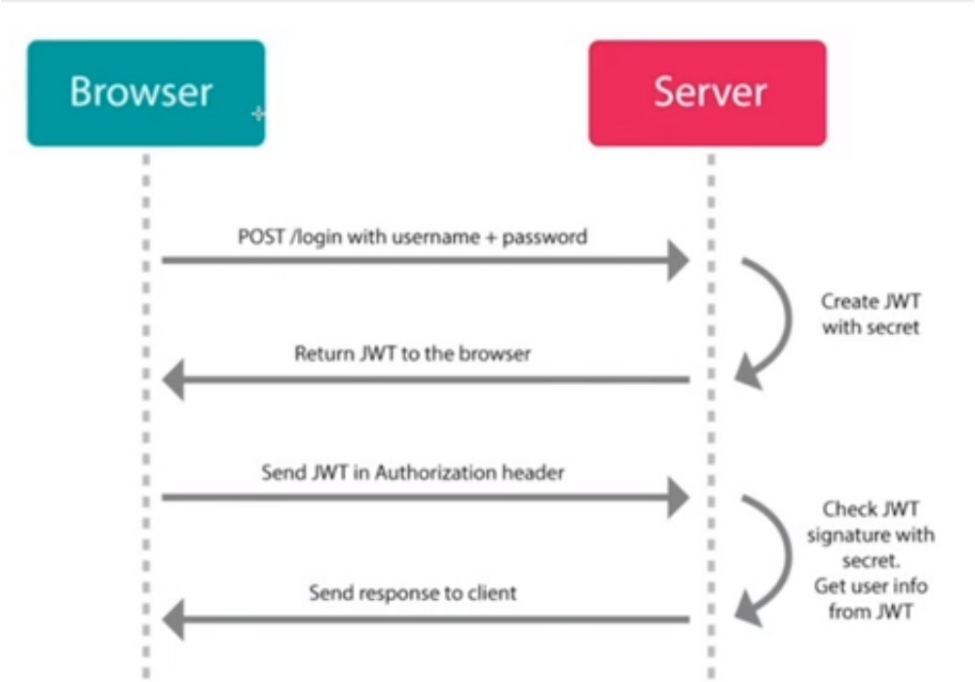
Consider a user has logged on to a client app.The user authentication was made and the client has been given with a token once it has been verified with the resource owner.Then the client uses the token generated to get the access token from the authorization server if the token given was authorized token.

Once the access token is received the client will request for the resources from the resource server and carry out the process and the client is provided with limited access only.



JWT:

Json Web Tokens(JWT) are tokens that are used in HTTP services involving two parties.



Difference between JWT and OAUTH:

JWT	OAUTH
1. A signed Token will be generated using the client credentials and it is used for further requests.	**1.** An Access Token is generated with the client_id and client secret and then the authorization code being generated and the token is used to access resources.
2. Used in a two party HTTP services	**2.** Used when more than two parties are involved.
3. It is more efficient and it is built using standard cryptography algorithms.	**3.** It provides only limited access and it is also generated using standard algorithms.

- Kishor Kumar
Msc Computer Science