Introduction to OAuth2.0

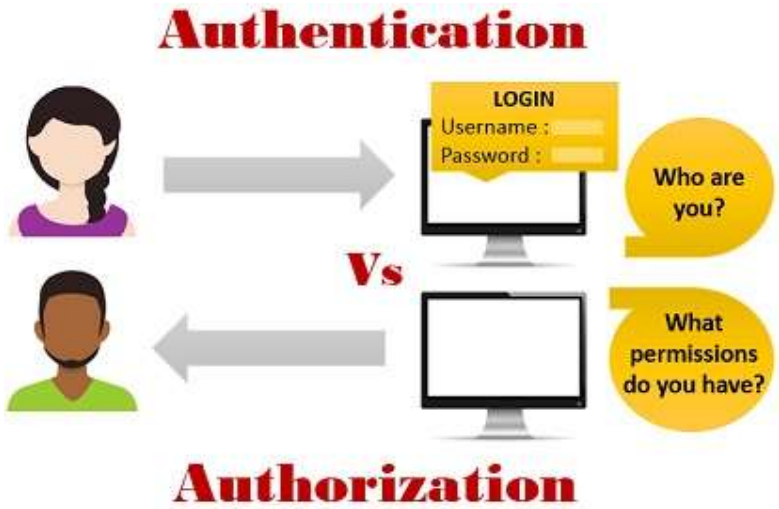
Some of the slides are taken from:

Understanding OAuth2.0, Amit Harsola, Wipro Technologies

https://www.slideshare.net/amitharsola/understanding-oauth-20

Authentication vs. Authorization

- Authentication
  - Confirming your own identity
  - The process of verifying who you are
- Authorization
  - Granting access to the system
  - Process of verifying what you have access to



Web Authentication

In a typical web authentication model, user owning the resource shares credentials with other applications to provide them access to their protected data

The above approach presents significant challenges for the resource owners

1. It requires sharing of passwords in clear text which third party applications stores for any future use

2. Any compromise of third party application results in compromise of user's password and its data

3. Resource access revocation is only possible by user through password change

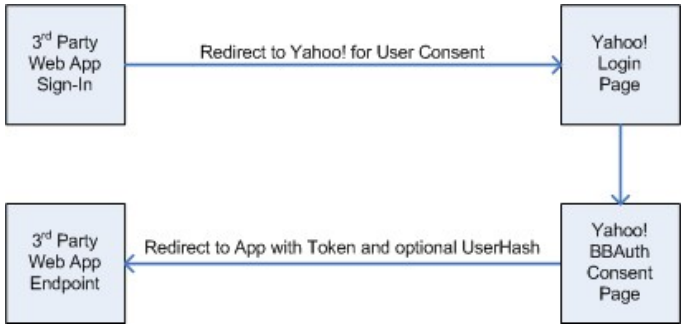
4. Third party applications have full access to user's data i.e. no data level or data scope access

Social Web Integration

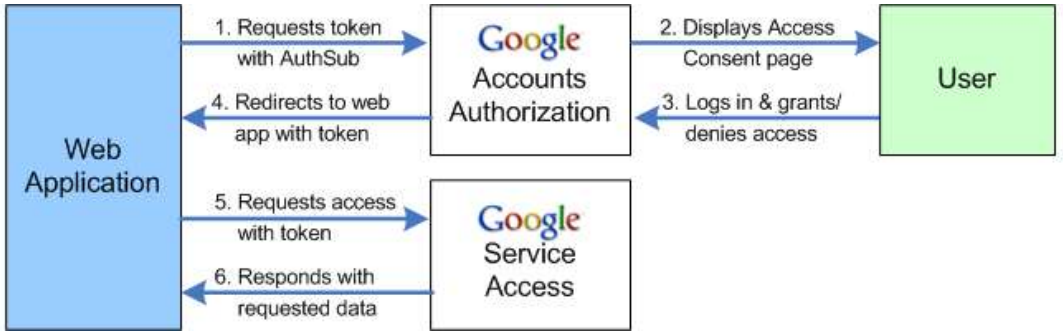
Several proprietary authorization protocols have emerged to address the integration problem i.e. AuthSub (Google), OpenAuth (AOL), BBAuth (Yahoo), Amazon Web Services API, etc

These proprietary protocols burdens the API consumers with implementations, all serving the same purpose i.e. web integration for exchange of protected data.

Internet Engineering Task Force (IETF) have proposed an OAuth protocol which integrates the commonalities and adopts the best practices of the proprietary Web authorization protocols into a single open standard



BBAuth



AuthSub

What is OAuth?

OAuth stands for “Open Authorization”

An open standard protocol that provides simple and secure authorization for different types of applications

A simple and safe method for consumers to interact with protected data

Allows providers to give access to users without any exchange of credentials
Designed for use only with HTTP protocol. It does not support any other protocol

Why OAuth?

OAuth is created by studying each of the proprietary protocols and extracting the best practices

It is flexible, compatible and designed to work with mobile devices and desktop applications

Provides a method for users to grant third-party access to their resources without sharing their credentials.

Provides a way to grant limited access in terms of scope and duration

Has support from big players in the industry

History

OAuth Core specification 1.0 was published in Dec 2007

To fix a security issue, a revised specification was published in June 2009

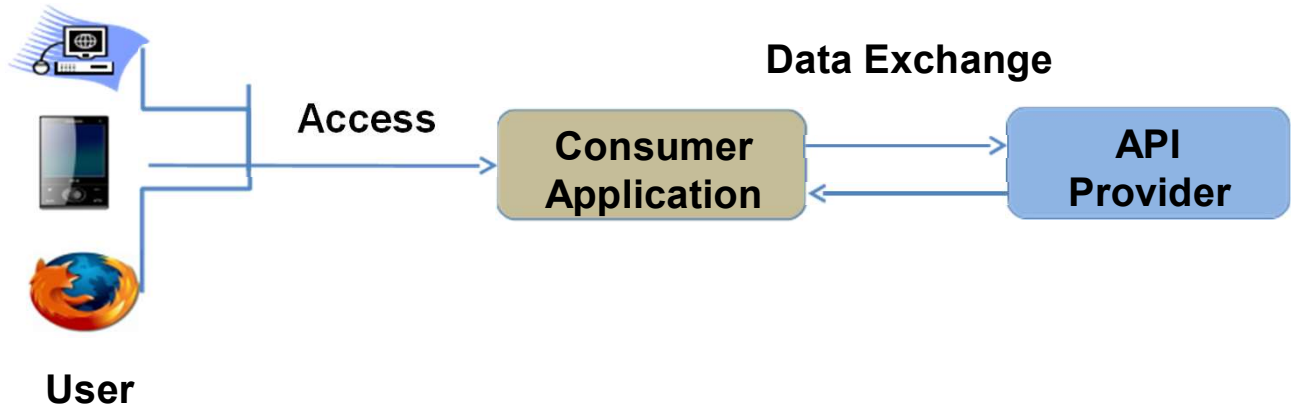
OAuth 2.0 is a completely new protocol which is not backwards compatible with previous versions. However, it retains the overall architecture and approach established by the previous versions.

Various Services on the Web already support OAuth 2.0

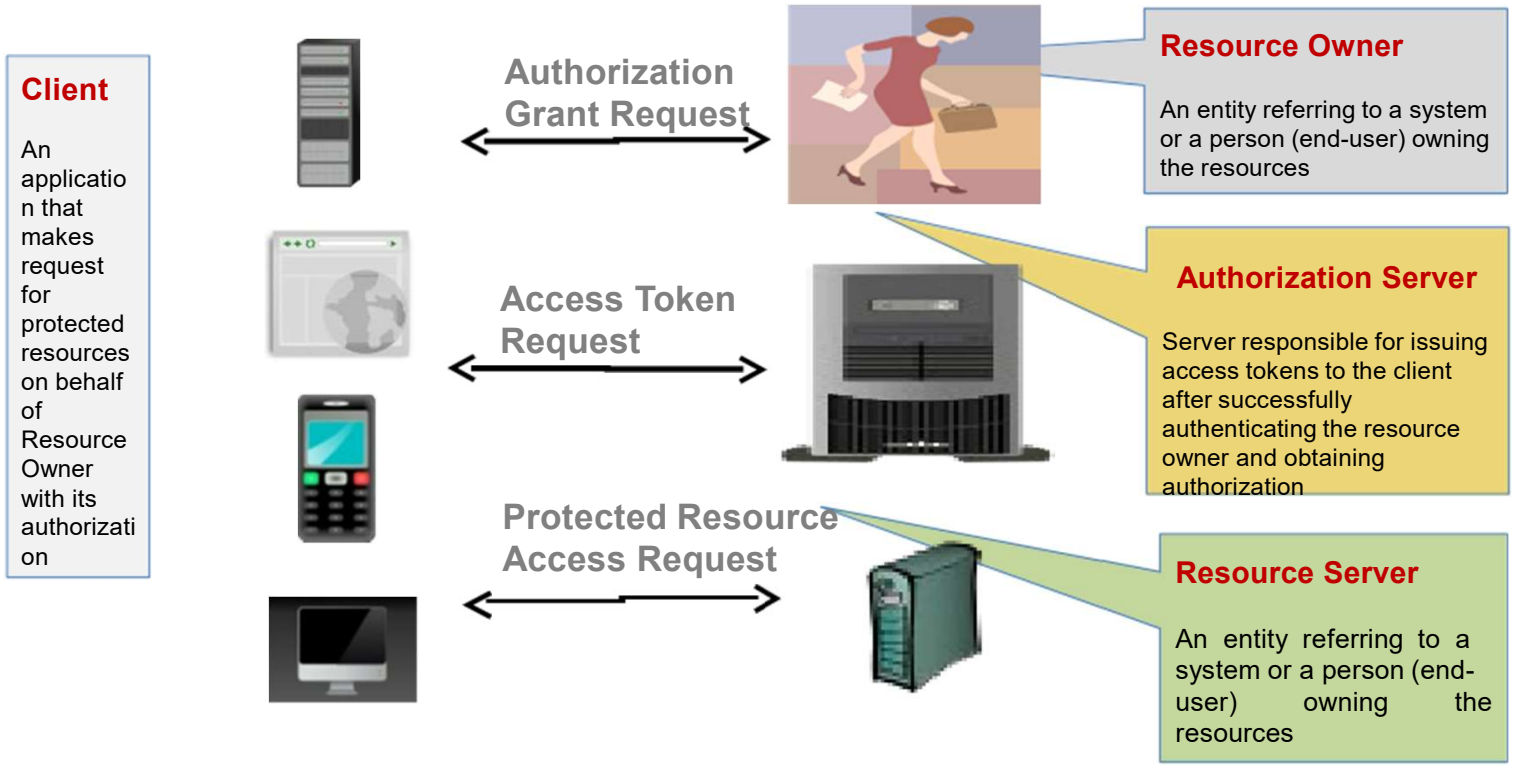
- Facebook's API
- LinkedIn
- Github
- Google
- Salesforce
- Windows Live

OAuth – Introduction

- User accesses consumer application which first gets user authenticated through API Provider application for any exchange of information
- Once authenticated, consumer application and Provider exchange tokens for authorization
- After successful authorization, consumer application gets access to users resources on Provider application



OAuth 2.0 – Overview

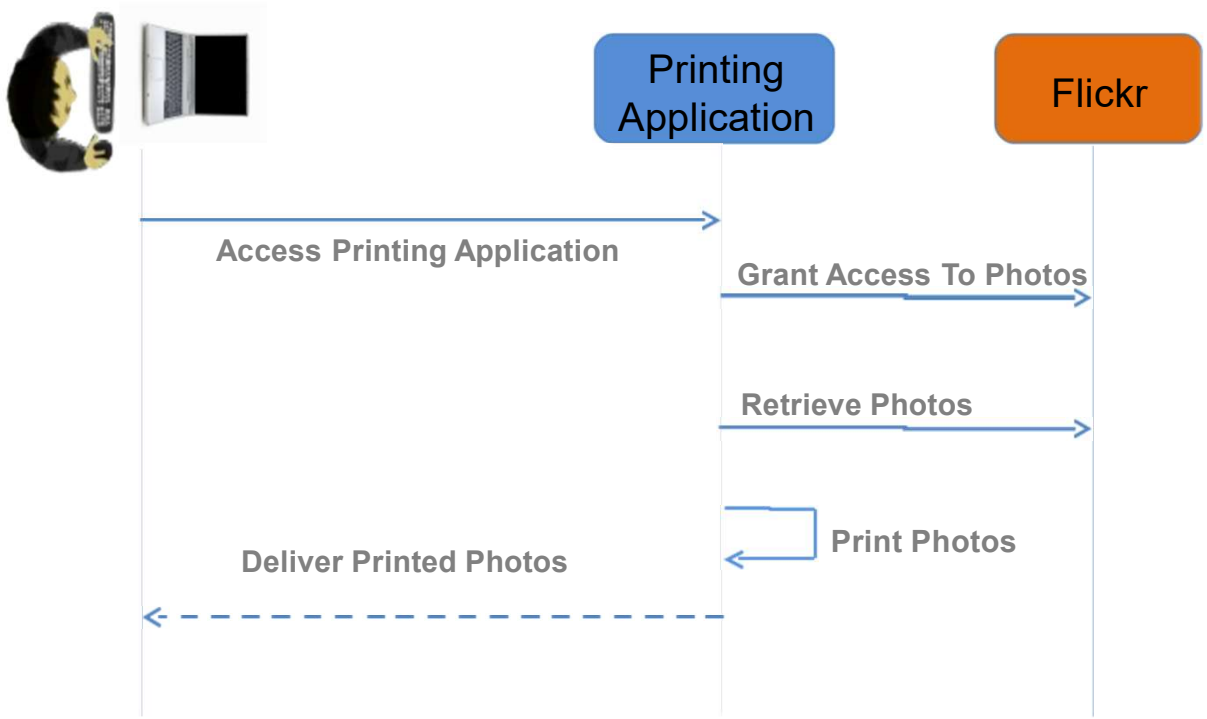


The authorization server may be the same server as the resource server or a separate entity

Use Cases – Social Portals

Social Portals

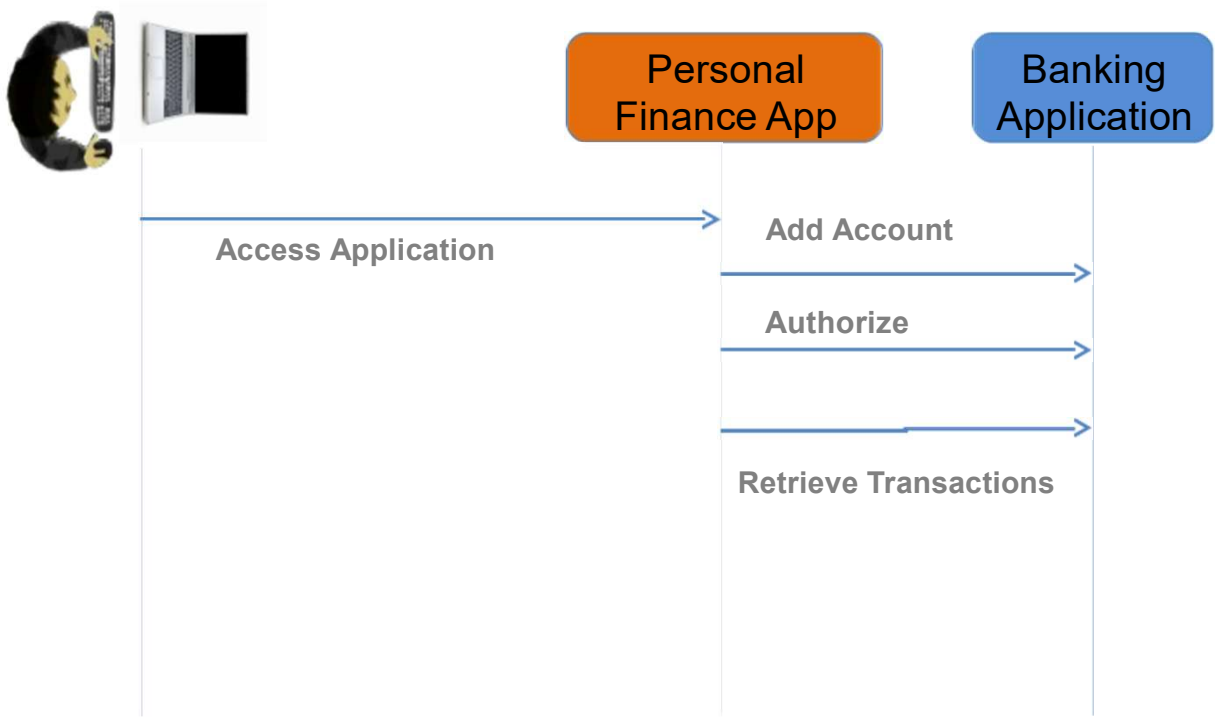
It is the most common use case where organization intends to leverage the users of Social Applications and APIs offered by them



Use Cases - Financial

Financial

Another use case of OAuth could be Personal Finance Management Applications. Banking users could authorize bank to share all banking transactions with Money Finance Application which would provide an holistic view of user's financials



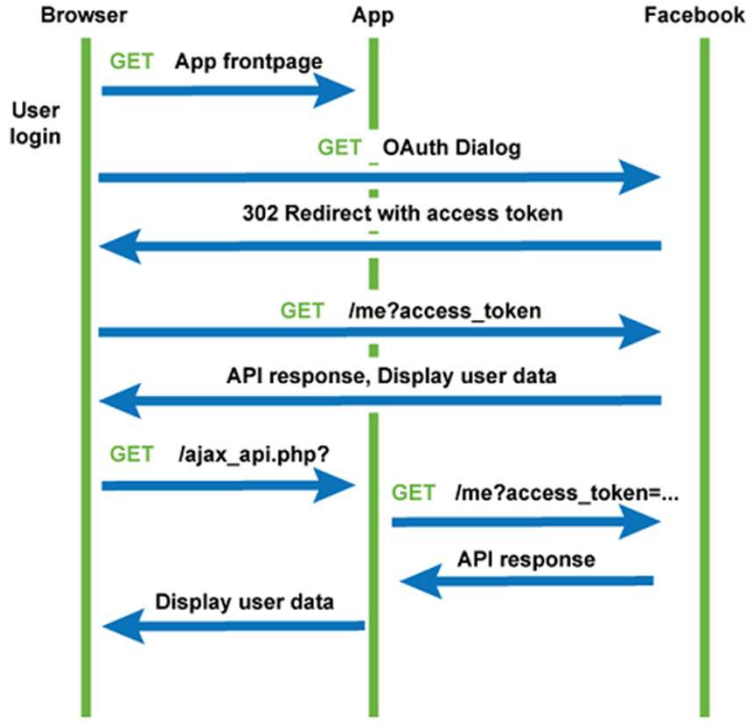
Use Cases – Facebook

Facebook OAuth

A secure, fast, and convenient way for users to log into your app, and for your app to ask for permissions to access data

Facebook Graph API

HTTP-based API that apps can use to programmatically query data, post new stories, manage ads, upload photos, and perform a wide variety of other tasks



How to Use Facebook OAuth

Configuring Facebook Login

https://help.sharetribe.com/sharetribe-go-managing-your-go-marketplace/third-party-sign-up-services/how-to-configure-facebook-login

Postman Demo