White Paper

Access Manager

OAuth 2.0: Securing APIs, Mobile, and Beyond

OAuth 2.0 is the standard for authorizing access to four major forces that are currently driving business innovation: cloud, social, mobile, and APIs.

This simple yet flexible protocol is useful in many ways. OAuth powers the billions of social logins that are performed every day. However, enterprises (not internet users) are driving OAuth's rise in popularity because it helps with real business scenarios by securing APIs, mobility and cloud.

This whitepaper covers:

- **OAuth 2.0 Overview**
- **Securing APIs and Mobile: How OAuth Helps**
- **OAuth Use Cases**
- **Challenges with OAuth 2.0 and How NetIQ Access Manager Helps**

by Haripriya Sivapatham,
Micro Focus® Engineering

NetIQ

OAuth 2.0 is a standard authorization framework for allowing third-party applications to access specific services and data on behalf of the user.

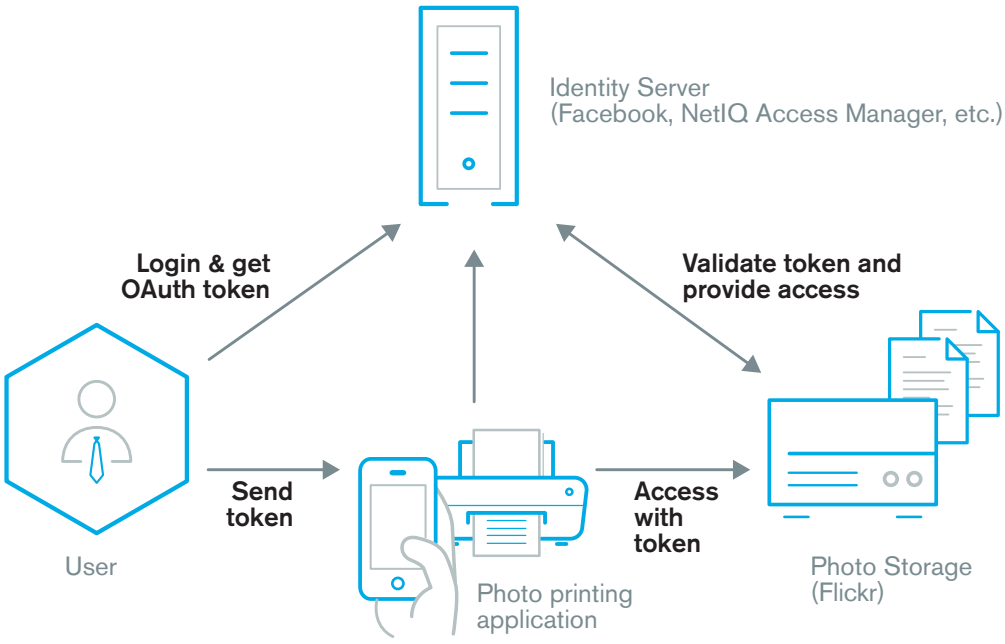
OAuth 2.0 Overview

What is OAuth 2.0?

OAuth 2.0 is a standard authorization framework for allowing third-party applications to access specific services and data. After users authenticate (log in), OAuth 2.0 determines which resources third-party applications can access and the actions these applications can perform on behalf of the user.

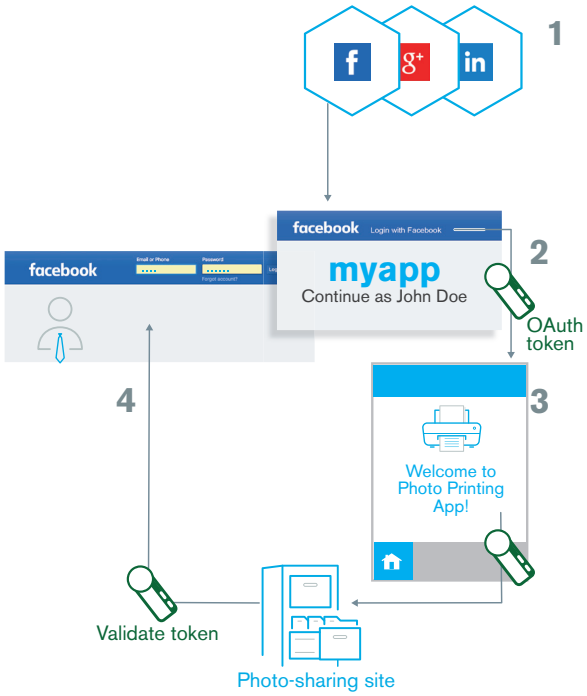
Let's take the example of a photo printing app that allows users to print their photos from Flickr. Photos on Flickr are accessible only when users are logged in. However the users cannot share their credentials with this photo printing app. Here is how OAuth 2.0 helps:

- User credentials are stored only on the Identity Server. When the users log in, they get an OAuth 2.0 token. Tokens are like permission slips and give certain access rights to the token bearer.
- The photo printing app can use an OAuth 2.0 token instead of user credentials to access the photo storage site (Flickr).
- Users can select the access rights for a token. For example, they can specify a token that allows read-only access to photos.



OAuth 2.0 in Action

Here is a behind the scenes look at how the printing app scenario works and the role that OAuth 2.0 plays:



Step 1: Authentication

User logs into social site. This is not part of OAuth 2.0 protocol.

The focus of OAuth 2 is only authorization and leaves authentication to the application (social site). OAuth 2 simply requires the user to be authenticated and it does not dictate the type of authentication to be used. Extensions to OAuth2 such as Open ID Connect (OIDC) can be useful for authentication and even for SSO.

Step 2: User Consent

OAuth 2.0 allows the user to decide what can be shared with the third-party application. An OAuth token will be created based on the rights to which the user consents.

Step 3: Get OAuth Token

The third-party printing app receives an OAuth bearer token from the social site. This token includes details about the access rights of the token bearer. The application can then use this token to access the photos on behalf of this user.

A token is analogous to a concert ticket.

- Like access tokens, a ticket provides limited access (one seat and not backstage), and is time bound.
- The ticket is sufficient to enter the arena. There is no need to provide any other details about you ("user credentials").
- You can give your ticket to your friend ("delegate access") and he can enjoy all the benefits in your place.

Step 4: Access Resource

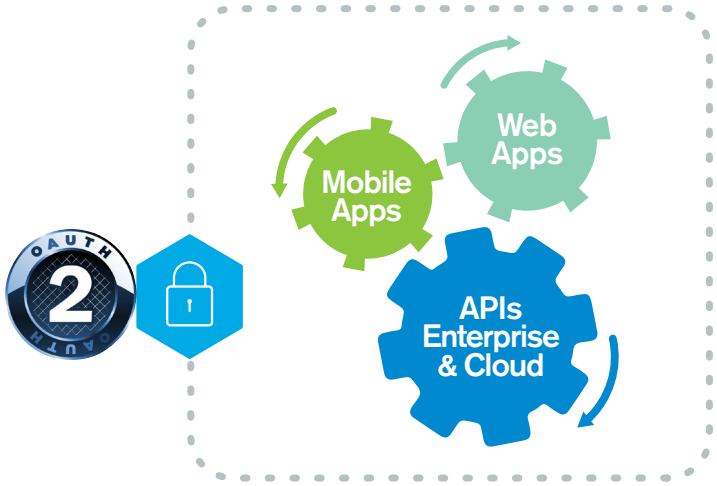
The printing app can now access the resource server (Flickr) using the token to get the user's data (photos).

This is a simplified example of how OAuth 2.0 works. There are different types of scenarios where OAuth 2.0 can be deployed, with four different protocol flows (which are called "grant types") for obtaining the access token. There are other kinds of tokens, too. For example, there are ID tokens that contain user details and refresh tokens that can be used to obtain new access tokens.

Enterprises that want to support diverse clients and reuse—rather than reinvent—available services are driving the current uptick in API development and use. As APIs become an ever greater part of the core business model, ensuring their security becomes critical

Securing APIs and Mobile: How OAuth 2.0 Helps

OAuth 2.0 is rapidly becoming the standard for securing access to APIs, mobile, and web applications.



Application programming interfaces (APIs) are the technical lynchpins for mobile, cloud, and Internet-of-Things (IoT). They provide a standardized mechanism for sharing services and data with third-party entities. Enterprises that want to support diverse clients and reuse—rather than reinvent—available services are driving the current uptick in API development and use. As APIs become an ever greater part of the core business model, ensuring their security becomes critical.

Key OAuth 2.0 Features

- **Delegated Access.** Before the advent of OAuth 2.0, third-party applications such as the printing app in the preceding scenario needed the users' credentials to access the social site on the users' behalves. However, allowing users to share their credentials with external applications presents an unacceptable security risk. OAuth 2.0's access tokens serve as a replacement for users' credentials. By delegating access, they allow secure collaboration.
- **Selective Access.** OAuth 2.0 provides fine grained access control so that users can decide who can access what protected resources and for how long. Another differentiator is that the user is in control, not the security administrator.
- **Revoke Access.** Users can revoke the access tokens that they give to third-party applications. This capability is especially useful for denying access to mobile applications that are running on lost or stolen devices.
- **Better security.** Time bound, randomly generated tokens always offer better security than do traditional passwords.

API Market is on Fire

Source: Forbes Magazine

70% of US organizations are actively using APIs

Source: IDC Mar 18, 2015

50% of B2B collaboration takes place through Web APIs

Source: IBM: API Economy Nov 2015

13 billion API calls are made per day to Twitter

Source: ProgrammableWeb

67% of people who do not use mobile banking cited security concerns as the reason for this.

Source: US Federal Reserve–Consumer and Mobile Financial Services Report, 2016

OAuth 2.0 Use Cases

MOBILE SECURITY

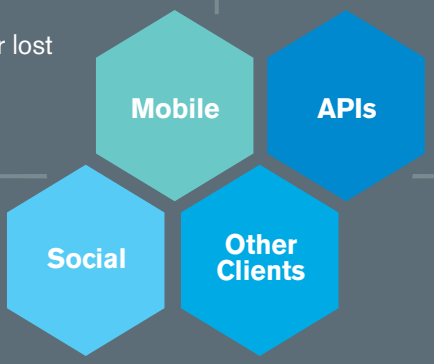
The number of downloaded mobile applications has now exceeded 100 billion. The trust level of these applications varies widely. Following are some of the OAuth features that help with mobile security:

- ✓ Works with existing authentication and ensures that all security rules, such as risk analysis, device fingerprinting, and so forth, are applied for mobile applications as well.
- ✓ Never exposes user credentials to third-party apps.
- ✓ Allows users to log in once–sessions are active even after restart (instead of storing user credentials on the device, an opaque OAuth 2.0 access token is used).
- ✓ Allows users to revoke access for lost devices.

API SECURITY

Enterprises have elevated APIs from a development technique to key business drivers. The following OAuth features are tailored for API security:

- ✓ Allows users to authorize applications while reusing current authentication mechanisms.
- ✓ Provides granular access control for representational state transfer (ReST) APIs.
- ✓ Allows delegated access so that credentials are not distributed to all API clients.
- ✓ Revokes access for compromised tokens.



SOCIAL LOGIN

OAuth was designed to meet social login requirements, it:

- ✓ Delegates identity and access management to social providers.
- ✓ Allows users to control the data they share with other websites.
- ✓ Lets users select the level of access to be allowed.
- ✓ Allows users to revoke access.
- ✓ Puts management in users' hands, as opposed to admin's hands.

OTHER CLIENTS

OAuth helps secure ReST APIs when they are accessed from different types of clients. It has specific authentication flows defined to cater to these clients, including:

- ✓ Browser-based applications.
- ✓ AJAX and JavaScript functions on the web page invoked by ReST APIs to leverage services exposed by the server.
- ✓ Machine-to-machine communication.
- ✓ Communication between a trusted client and a server when no user is involved.

NetIQ Access Manager provides a complete package to help deploy OAuth 2.0.

Challenges with OAuth 2.0 and How NetIQ Access Manager Helps

NetIQ® Access Manager™ provides a complete package to help deploy OAuth 2.0 and to implement various levels of security for the enterprise.

- **OAuth 2.0 is only a piece of the enterprise security puzzle**
  OAuth 2.0 alone cannot meet all the security requirements of an enterprise. Nonetheless, it is part of the security equation and must be included to satisfy a diverse access framework. For example, Security Assertion Markup Language (SAML) 2 can be used for authentication and OAuth 2.0 can be used for authorization by converting SAML's assertion into an OAuth 2.0 access token.

  NetIQ Access Manager provides various authentication options, including multi-factor and step-up options. It also provides advanced risk detection, device fingerprinting, and fine-grained policy-based access. In addition, it offers complete OAuth 2.0 support and acts as the OAuth 2.0 authorization server. In short, NetIQ Access Manager provides an end-to-end solution to completely secure the enterprise.
- **OAuth 2.0 provides the bottom tier of security: user controlled access**
  OAuth 2.0's design of user-driven access control is not sufficient for an enterprise. Enterprises require multiple levels of security. Administrators enforce enterprise level security policies, while user-controlled access is for user convenience.

  NetIQ Access Manager provides a full-fledged policy framework that allows administrators to configure who can access what and to assess users' risks, their devices, and so forth before the control even goes to the user.
- **OAuth 2.0 is a moving target**
  Newer specifications are coming up to ease integrations.

  NetIQ Access Manager provides complete OAuth 2.0 and OpenID Connect (OIDC) support with respect to the current request for comment (RFC) specification. Major enterprises have already applied this solution to meet their needs. Hence, NetIQ is committed to enhancing the solution as needed and to keeping up with new specifications as they emerge.
- **Enterprises already have a large number of legacy applications**
  Legacy applications must be OAuth enabled to work with modern OAuth 2.0 clients.

  NetIQ Access Manager caters to all of the established enterprise applications that are transitioning to OAuth 2.0. It acts as a bridge between OAuth clients and legacy applications. Modern OAuth 2.0 clients can now access legacy resources while Access Manager takes care of translating the OAuth 2.0 tokens into the kinds of authentication required by backend web servers.

Next Steps

Learn more about OAuth 2.0 support and view the sample code at: **www.netiq.com/communities/cool-solutions/oauth2-reference-for-access-manager/**

NetIQ Access Manager provides a comprehensive solution for securing your enterprise APIs, mobile deployments, federated applications, legacy systems, and Software as a Service (SaaS) and Platform as a Service (PaaS) offerings. To learn more about NetIQ Access Manager, go to: **www.netiq.com/accessmanager**

www.netiq.com

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

For a complete list of our offices
in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit: www.netiq.com/contacts