文章编号:1005-6033(2012)17-0080-02　　收稿日期:2012-05-04

# Web 2.0 时代的安全框架——OAuth

朱宇飞

(长治市科技信息中心,山西长治,046000)

**摘　要**:Web 2.0 时代,Web 服务成为互联网平台上服务整合与集成的基础。随着互联网巨头们尤其是社交网站以 API 的方式开放其服务供第三方调用,安全框架(认证与授权)日益成为突出的问题。在此背景下,OAuth 应运而生,现已成为 Web 服务(API)授权方面的事实标准。介绍了 OAuth 的基本概念及 OAuth 2.0 定义的重要流程。

**关键词**:Web2.0;OAuth;安全框架;认证;授权;访问令牌

**中图分类号**:TP393.092.1　　**文献标识码**:A

## 1　OAuth 的概念及应用概况

OAuth 是一个用来实现授权（Authorization）功能的开放标准。它允许用户将保存在一个网站上的私有资源(照片、视频、联系人等)开放给另一个网站,而无需向该网站提供自己的用户名和密码。在 OAuth 模型中,保存用户资源的网站称为“资源提供者”(Resource Provider),用户为“资源所有者”(Resource Owner),需要访问资源的网站称为资源“消费者”(Consumer)或“客户”(Client)。举例来说,用户(“资源所有者”)可能将照片上传到某个照片存储网站（“资源提供者”），而通过另一个照片冲印网站(“资源消费者”)冲印照片。如果没有 OAuth,照片冲印网站需要用户在照片存储网站的用户名和密码去获取用户的资源，但这样一来,照片冲印网站将可以控制用户的所有资源,用户无法对其进行限制,除非修改密码。用户对照片冲印网站是要么完全信任,要么完全不信任。在实际应用中,更多的时候是介于这两个极端之间,比如用户希望照片冲印网站获取自己的照片,但不可以获取自己的其他资源(视频、联系人等)。OAuth 通过向资源“消费者”发放“访问令牌”(Access Token)解决这个问题。每个“令牌”授权特定网站(如照片冲印网站)在特定时间内(如接下来两小时)获取特定资源(如仅照片)。这样用户无需泄露自己的用户名和密码,就可以授权某个资源“消费者”网站获取自己在另一个“资源提供者”网站存放的资源,并可以随时取消这一授权。

OAuth 随着 Web 服务和社交网站的迅猛发展应运而生。一方面，作为 Web 2.0 时代的重要特征之一,Web 服务成为互联网平台上服务整合与集成的基础,Web 服务及应用如雨后春笋般大量出现;另一方面,具有社交功能的网站成为这个时代的重要推手。社交功能的本质促使这些网站以 Web 服务的形式开放自己的服务,安全框架(认证与授权)日益成为突出的问题。可以说,OAuth 的出现,社交网站功不可没。Twitter,Facebook,Google 等都是 OAuth 规范的重要参与者和制定者。现在,OAuth 已成为 Web 服务(API)授权方面的事实标准,除了前面提到的,MSN,QQ,新浪等都已实现 OAuth。

2010 年 4 月,OAuth 1.0 协议作为 RFC 5849 发布。之后,该版本被发现存在安全缺陷,版本 1.0a 用来解决此问题。OAuth 2.0 是下一代 OAuth 协议,与 OAuth 1.0 不兼容。OAuth 2.0 着重简化客户端开发,同时为 Web 应用、桌面应用、移动应用及起居室设备提供不同授权流程。截至 2011 年,Facebook 的新 Graph API 仅支持 OAuth 2.0，是该新规范最大的实现。另外,Google 和 Microsoft 都为其 API 添加了 OAuth 2.0 实验性支持。

图 1 是 OAuth 协议所涉及的 4 种角色之间的抽象交互模型(“资源提供者”进一步划分为“资源服务器”和“授权服务器”),包含以下步骤:

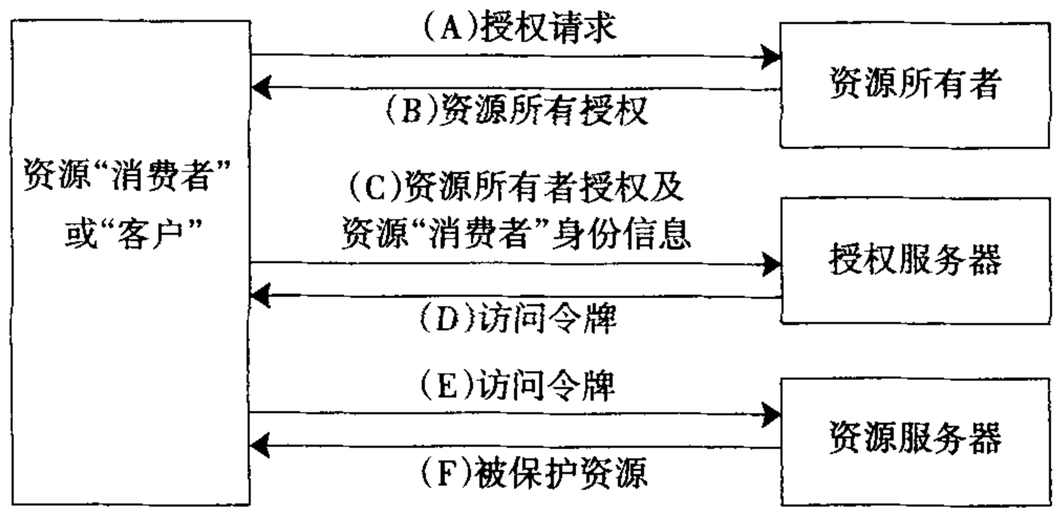


图 1　OAuth 协议所涉及的 4 种角色之间的抽象交互模型

(1) 资源“消费者”或“客户”请求资源所有者授权。授权请求可以直接发给资源所有者,或更安全地经过一个中介,如授权服务器。

(2)资源“消费者”或“客户”接收到资源所有者的授权。授权类型取决于授权服务器所支持及资源“消费者”或“客户”使用的方法。

(3)资源“消费者”或“客户”从授权服务器获取“访问令牌”。资源“消费者”或“客户”需要提供自己的身份信息(由授权服务器预先分配)并提供在上一步得到的授权,授权服务器依靠这些信息对其进行认证。

(4)授权服务器验证资源“消费者”或“客户”的身份信息及用户对其授权,如果通过,发放一个“访问令牌”。

(5)资源“消费者”或“客户”从资源服务器获取被保护的资源,提供“访问令牌”以进行认证。

(6)资源服务器验证“访问令牌”,如果有效,处理资源获取请求。

## 2 OAuth 2.0 定义的重要流程

### 2.1 授权流程

OAuth 2.0 支持 4 种授权流程：授权码流程(Authorization Code flow)、隐含授权流程(Implicit Grant flow)、资源所有者密码流程(Resource Owner Password Credentials flow)、资源"消费者"认证流程(Client Credentials flow)。

(1)授权码流程(Authorization Code flow)。当资源"消费者"或"客户"是一个第三方服务器或 Web 应用时，使用授权码流程。在此模型中，Web 服务器访问"资源提供者"网站上的资源。资源"消费者"没有用户的用户名和密码信息。

第一，用户浏览器连接到一个资源"消费者"的 URL，资源"消费者"将用户重定向到授权服务器，该重定向包含资源"消费者"标志(client id)，请求(scope - 所请求的权限)，以及一个指回资源"消费者"的 URL(重定向 URL)。

第二，授权服务器要求"资源所有者"进行授权，可能需要对"资源所有者"进行认证，如验证用户名和密码，并确认资源"消费者"所请求的操作。授权成功后，授权服务器将用户重定向回资源"消费者"(通过资源"消费者"提供的重定向 URL，并在该 URL 中添加一个授权码)。

第三，资源"消费者"提供的重定向 URL 一般指向一段服务器端脚本，该脚本通过发一个 POST 请求到授权服务器以获得"访问令牌"(Access Token)。POST 请求应使用 client secret 生成签名，并提供上一步收到的授权码(证明"资源所有者"确实授权了该请求)。授权服务器将返回"访问令牌"(Access Token)及其过期时间。

(2)隐含授权流程(Implicit Grant flow)。当用户浏览器直接访问"资源提供者"网站上的资源时，使用隐含授权流程。这种模型针对富 Web 应用或移动应用，不使用 client secret。

第一，用户浏览器连接到授权服务器的一个 URL。这可能是一个直接连接，也可能是资源"消费者"做的重定向。请求包含资源"消费者"标志(client id)、目标范围以及重定向 URL。如果授权服务器接受此请求，将重定向到资源"消费者"提供的重定向 URL，并在该 URL 后包含"访问令牌"(Access Token)及其过期时间(在"#"后)。

第二，虽然重定向 URL 指向资源"消费者"服务器，资源"消费者"服务器端不会处理它。该 URL 可能用来加载一段 Javascript 代码，这些代码从 URL 种获得"访问令牌"并使用它。或者，移动应用可以捕获到此重定向，提取出"访问令牌"并使用它。这时，重定向 URL 可能只是指向静态内容。

(3)资源所有者密码流程(Resource Owner Password Credentials flow)。当资源所有者完全信任资源"消费者"时，使用资源所有者密码流程。这种模型资源"消费者"将获得用户的用户名和密码，然后直接传给授权服务器以获得"访问令牌"。这一流程可用于迁移旧的用户名/密码认证模式。

(4)资源"消费者"认证流程(Client Credentials flow)。资源"消费者"认证流程完全基于资源"消费者"的 secret 获取"访问令牌"。

### 2.2 访问被保护资源

资源"消费者"或用户浏览器(隐含授权流程)获得"访问令牌"后，就可用它访问被保护的资源。OAuth 2.0 定义了两种标准方式发送"访问令牌"，具体应用可以定义更多的方式。

#### 2.2.1 无记名令牌(Bearer Token)

"访问令牌"应该放在 Authorization HTTP header 中，或者放在 POST 请求体中。作为 GET URL 参数是最不安全。

#### 2.2.2 MAC

MAC(消息认证码：Message Authentication Code)根据请求计算并放在 Authorization header 中发送。资源提供者收到请求时重新计算 MAC 并进行比较。"访问令牌" 应放在 Authorization HTTP header 里。

### 2.3 刷新令牌(Refresh Tokens)

在授权码和资源所有者密码流程中，授权服务器可以选择产生一个"刷新令牌"。这个"刷新令牌"用来获得新的"访问令牌"而无须重新授权。

现在，OAuth 已是 Web 服务(API)安全认证与授权的事实工业标准。如前所述，著名的社交网站都在大力推动并已实现 OAuth，新的网站如果想在 Web 2.0 的舞台上有所表现，也须支持 OAuth。因为 OAuth 保证了在提供开放资源(API)的同时，访问者必须由适当的授权。对用户来说，可以在不同的网站或应用中使用保存在特定网站上的资源，简化了管理，改进了体验。可以说，OAuth 必将有力地推动互联网资源开放共享的发展，在为用户提供丰富的互联网服务的同时，保证其安全性。

(责任编辑：李 敏)

**第一作者简介**：朱宇飞，男，1974 年 5 月生，1996 年毕业于杭州电子工业学院，助理研究员，长治市科技信息中心，山西省长治市城西路 28 号，046000.

# The Security Framework in Web2.0 Age

**ZHU Yu-fei**

**ABSTRACT:** In Web2.0 age, Web service has become the foundation for services' configuration and integration on Internet platform. Along with that the giants of Internet, especially the social networks, open their services for third party's calling with API mode; the security framework (authentication and authorization) has become an increasingly prominent problem. Under such background, OAuth emerges at the right moment and has become the de facto standard in aspect of Web service's API authorization. This paper introduces the basic concepts of OAuth and the important process defined by OAuth 2.0.

**KEY WORDS:** Web2.0; OAuth; security framework; authentication; authorization; access token