基于国内开放平台的Oauth认证框架研究

刘 镝[1,2] 张智江[3,4] 张 尼[4]
1 中国联合网络通信集团有限公司博士后工作站 北京 100033
2 北京邮电大学 北京 100876
3 中国联合网络通信集团有限公司 北京 100033
4 中国联通研究院 北京 100032

摘 要 首先对现有不同种类的国内开放平台的Oauth认证授权应用实例进行归纳比较。然后对开放平台中Oauth认证机制进行了分析和讨论，如对Oauth2.0认证体系、认证角色第三方应用开发者、普通用户、鉴权服务器、资源服务器进行了功能分析，并分析了它们之间的相互信任模型。最后以人人网Oauth2.0应用为例，详细描述了第三方应用开发者、用户在开放平台中授权、认证的过程。

关键词 Oauth2.0；Oauth1.0；认证框架

引言

随着互联网2011开放元年的到来，互联网厂商纷纷推出各自的开放平台，如腾讯开放平台、新浪微博开放平台、百度框计算搜索开放平台、淘宝TOP电子商务开放平台、360开放平台、人人网开放平台、盛大开放平台等。上述开放平台将各种不同的网络服务封装到一系列计算机易于识别的数据接口当中，并开放这些接口，由此网站不仅可以提供简单的网页接入，而且可以进行复杂的数据交换。厂商通过开放平台的理念将网站转变成为带有操作系统的开发平台。这样，第三方开发者可以基于开放平台的开放API开发各种各样的应用，构造出一个宏大的生态圈，吸引到更多的第三方开发者和独立软件提供商到该平台下发展，最终实现开放平台厂商与第三方开发者双赢的目的。

目前，开放平台的类型分为四类：1）社交类，如开心、人人、新浪微博平台；2）电子商务类，如淘宝TOP开放平台，腾讯支付通开放平台；3）搜索类，如百度开放平台；4）综合性开放平台，如腾讯开放平台、360开放平台等。

在构建平台过程中，用户与第三方应用、开放平台之间相互信任、交互的安全性是平台商需要考虑的因素。目前，业内开放平台用户身份信任机制主要采用Oauth授权方式。Oauth授权方式为客户端提供了一种代表资源拥有者访问受保护资源的方法[1]。Oauth协议是由IETF起草，目前最新版本为Oauth2.0第21版[2]。在客户端访问受保护资源之前，它必须先从资源拥有者获取授权，然后用访问许可交换访问令牌。客户端通过向资源服务器出示访问令牌来访问受保护资源[3]。

1 国内开放平台Oauth2.0应用实例分类

正如引言中所述，目前国内开放平台可归纳为四类。按照此分类方式，表1归纳了现有国内开放平台的Oauth应用。

由表1看出目前国内现有开放平台用户认证方式解决方案均为Oauth授权方式，但版本有所不同。大多数开放平台采用了较新的Oauth2.0版本，也有部分厂家采用了Oauth1.0a版本，或者两种版本共用。

对于第三类电子商务开放平台(以淘宝TOP开放平台

表1 各类开放平台Oauth应用总结

平台名称		Oauth授权版本	版本使用情况
社交类开放平台	人人网开放平台	Oauth2.0	率先在国内采用Oauth2.0授权方式
	开心网开放平台	Oauth1.0a	采用OAuth1.0a与Oauth2.0方式相结合为第三方网站/客
		Oauth2.0	户端提供连接服务
	新浪微博开放平台	Oauth1.0a	Oauth2.0登录接口目前仅对站内应用开放
		Oauth2.0	
搜索类开放平台	百度连接开放平台	Oauth1.0a	授权方式除采用Oauth1.0a，亦可采用类似Facebook connect专有授权机制
电子商务类开放平台	淘宝TOP开放平台	Oauth2.0	Oauth2.0第一步获取授权码，可选择正式环境与沙箱环境
综合类开放平台	腾讯开放平台	Oauth1.0a	腾讯微博API使用OAuth 1.0a版本

为例），在实施Oauth授权方式的过程中，考虑到安全问题，平台建立了沙箱机制(Sandbox)[4]。用户在获取授权码之后，可以选择正式环境完成认证过程，也可以选择沙箱模拟环境。沙箱环境是一个虚拟系统程序，模拟线上真实的电子商务平台环境，第三方应用用户可以在更加友好易用的测试环境中完全仿真地测试淘宝开放平台提供的接口功能。例如，不限制调用API的权限，不必使用真实的支付宝付款就能完成交易测试，在宝贝详情页面取消嵌入flash的限制等。因此，买家或卖家用户可以利用该环境熟悉TOP开放平台的运行环境，消除操作陌生感，提高用户体验。沙箱环境与正式环境所使用的域名不同，而且该环境中没有数据，因此不能获取报表。

2 开放平台中Oauth认证机制

2.1 开放平台中的身份认证体系

对第三方客户端或用户进行身份认证是开放平台安全体系中的重要内容。开放平台对每一次访问请求都需要进行独立的身份认证。目前，针对网络用户的身份认证有很多解决方案，而对于开放平台而言，Oauth2.0授权方式是目前广泛采用的一种解决方案。其基本思路就是由第三方客户端将用户重定向至开放平台的定制网页，用户在登录后完成身份认证并生成授权令牌，然后由开放平台重定向用户至第三方客户端并携带访问令牌，然后第三方客户端就可凭借该令牌，以用户身份访问平台开放的应用接口。

2.2 开放平台中Oauth2.0系统角色

为了详细认识Oauth2.0认证方式开放平台中网元间的相互信任机制，首先分析开放平台中的系统角色。

1）网站：提供数据交换或服务的站点，普通用户可以利用账户密码登录该网站进行业务操作。

2）第三方客户端：第三方应用系统通过开放平台入口，访问内部服务，从而完成跨域的业务整合。例如，第三方开发者为新浪微博开放平台开发的应用“育儿官方微博”，可以使用自己的域名，独立运行在该第三方服务器上，通过远程API调用完成业务功能。

3）用户(资源拥有者)：即网站用户，他们可能会使用第三方应用访问自己的数据，或完成该网站应用业务。在第三类电子商务开放平台中，用户可能需要分为两类。①业务提供方，利用开放平台和第三方应用向业务接收方提供业务，如淘宝TOP卖家。②业务接收方，利用开放平台和第三方应用接收业务提供用户提供的业务，如淘宝TOP买家。

4）鉴权服务器：开放平台中用于鉴别第三方客户端业务请求及颁布访问令牌的服务器。

5）资源服务器：用于接收第三方客户端发送的访问令牌，并返回第三方应用所需的相关数据，或返回相关应用业务的结果。

6）服务接口：站点内部某个提供数据交换或者完成业务应用的服务接口。一般使用HTTP协议进行访问，数据格式如SOAP、XML等。

2.3 Oauth2.0模型分析

Oauth2.0认证框架用户授权流程大致如下。

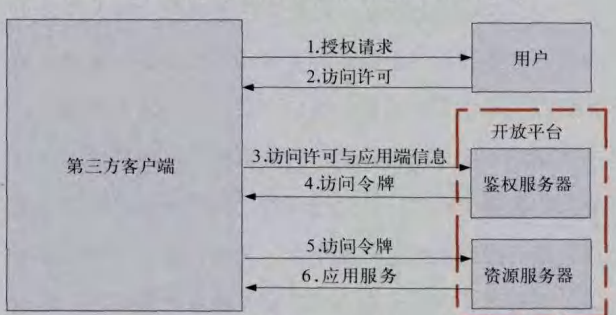

图1 Oauth2.0框架流程

图1中展示了Oauth2.0授权方式的大致流程，其中开放平台包括鉴权服务器、资源服务器。针对以上流程，下面进行逐一介绍。1）授权请求：第三方客户端直接发送到网站用户请求给予授权，或者间接通过授权服务器这样的中介请求授权。2）访问许可：若用户同意授权，则第三方客户端从用户端接收一个用户访问许可，该许可代表由资源服务器提供的授权。3）访问许可与第三方应用端信息：第三方客户端使用自己的私有证书在鉴权服务器上进行鉴权认证，出示访问许可，来请求访问令牌。4）访问令牌：鉴权服务器验证第三方客户端私有证书和访问许可的有效性，若验证通过，则颁发访问令牌。5）发送访问令牌：第三方客户端通过出示访问令

牌向资源服务器请求获取受保护的资源。6）应用服务：资源服务器验证访问令牌的有效性，若验证通过，则回应该请求，分发给第三方客户端需要的受保护数据。

3 Oauth2.0授权方式应用实例

本章参照图1的Oauth2.0授权模型原理，以社交类平台人人网Oauth2.0应用为例，具体分析开放平台中用户及第三方应用用户注册、认证流程。

人人开放平台应用种类可分为三类。1）站内应用。该种应用又分为web站点应用(如开心农场)与wap网站应用(如开心农场wap版)。Web站点及wap站点应用都集成在人人网内部使用；2）网站应用。亦分为web站点应用与wap站点应用，这两种应用都位于独立于开放平台本身的网站，并注册为该平台的应用，如糯米网；3）桌面客户端应用。运行在电脑上的客户端软件也可注册成为开放平台应用，并提供一些功能让人人网用户使用，如：美图秀秀客户端软件就是一个将本地美化过的图片上传到人人网上的桌面客户端应用。以上三种类型的人人网应用访问都需要利用Oauth2.0进行用户身份认证。下面将详细介绍具体过程。

3.1 第三方用户应用注册

当第三方应用用户注册申请一个应用后，则从平台获得一对API key(相当于client_ID)与secret(client-secret)。例如，应用ID155097，其对应的API key为db8c2e8f61fc4a81bddb9e5433608709，Secret key：4eefabfa78c74ba4a96f73e755a6ff1e。生成该Secret key的目的是保证数据通信的安全性。

3.2 第三方应用用户授权页面方式

目前人人网站主要使用的模式为服务端流程(Web sever flow)，该模式适用于有Web服务器的应用，希望从自己的Web服务器发送API调用请求的应用，如Web站点、有Web服务器支持的客户端应用等。该模式主要体现在第三方应用用户与鉴权服务器之间的身份验证。

第一步：获取Authorization Code。从人人网用户浏览器提交请求，浏览地址被重定向到鉴权服务器(https://graph.renren.com/oauth/authorize)，请求过程中至少携带3个必要参数，即相当于第三方客户端的credentials。

1）client_id：注册应用时获得的API Key；

2）response_type：若应用类型为Web应用时，此值固定为“code”；

3）redirect_uri：授权后要回调的URI，即接受code的URI。

该步骤相当于图1模型中的第一步。

第二步：使用Authorization Code换取Access Token。在接收Authorization Code的第三方应用程序中发送请求至鉴权服务器https://graph.renren.com/oauth/token，并且传递5个参数。

1）grant_type：使用Authorization Code作为Access Grant时，此值为“authorization_code”；

2）code：Authorization Code(第一步已经获取)；

3）client_id：第三方应用的API Key；

4）client_secret：第三方应用的Secret Key；

5）redirect_uri：必须与获取Authorization Code时传递的“redirect_uri”保持一致。

该步骤相当于图1模型中的第三步。

第三步：返回Access token。若参数无误，鉴权服务器将返回一段JSON文本，包含4种参数。

1）access_token：要获取的Access Token；

2）expires_in：Access Token的有效期(秒)；

3）refresh_token：用于刷新Access Token的Refresh Token；

4）scope：Access Token最终的访问范围，即用户实际授予的权限列表(用户在授权页面时，有可能会取消掉某些请求的权限)。

若请求错误，鉴权服务器将返回一段JSON文本，包含“error”、“error_description”和“error_uri”。

该步骤相当于图1模型的第4步。

4 结束语

本文首先对社交类、搜索类、电子商务类、综合类共四类的国内开放平台Oauth认证授权应用实例进行了