ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.8, No.22, August 2012.

E-mail: xsjl@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

第三方应用与开放平台OAuth认证互连技术研究

刘大红[1,3],刘明[2]

(1.同济大学 软件学院,上海 200000;2.宁夏大学 数学计算机学院,宁夏 银川 750021;3.银川市职业技术教育中心,宁夏 银川 750021)

摘要:针对国内开放平台的用户验证和授权问题,分析了OAuth服务中第三方应用、普通用户、授权服务器及资源服务相互认证模型。最后以腾讯开放平台为例,对其接入规范和腾讯OpenAPI进行研究,实现并验证了BBS站点与腾讯开放平台的账号互通功能。

关键词:OAuth;账号互通;开放身份认证;OpenAPI

中图分类号:TP393 文献标识码:A 文章编号:1009-3044(2012)22-5367-03

Research on the Third Party Applications and Open Platforms Interconnection Based on OAuth Authentication

LIU Da-hong[1,3], LIU Ming[2]

(1.School of Software Engineering,Tongji University,Shanghai 200000,China; 2.School of Mathematics and Computer Science,Ningxia University, Yinchuan 750021,China; 3.Yinchuan Vocational and Technical College,Yinchuan 750021,China)

Abstract: In face of user validation and authorization problems.Analyse the authentication model among third party applications,users,authorization servers and resource servers in OAuth service.In the end,take Tencent open platform for example,research it's access standard and OpenAPI,realise and verify account interchange function between a BBS site and Tencent open platform.

Key words: OAuth; account interconnection; open identity authentication; OpenAPI

开放平台代表了互联网数据开放的发展趋势,国内外IT巨头先后推出了自己的开放平台以实现战略联盟与抗衡,如腾讯开放平台、新浪微博开放平台、百度开放平台、人人网开放平台及360开放平台等。开放平台可以实现社交网站之间用户账号互通,减少用户登录操作;第三方应用可以基于社交网站的开放接口OpenAPI对授权数据进行应用开发,实现战略共赢。OAuth协议为开放平台中用户资源授权与身份验证问题提供了一个安全、开放的标准。

1 基于OAuth协议的认证授权技术

1.1 OAuth协议

OAuth(Open Authentication)是一个开放的认证协议,其可以在不让第三方接触用户名和密码等敏感信息的前提下,完成第三方对用户资源访问请求的认证授权。2010年OAuth1.0被IETF认定为互联网标准协议[1]。目前,国内外大多数开放平台采用了OAuth2.0安全认证机制,同时提供OAuth1.0的安全认证支持。由于它的简易性、安全性和开放性[2],OAuth已成为开放资源授权事实上的标准。

简单性,无论OAuth服务提供者还是应用开发者,OAuth易于理解与使用;业界提供了OAuth的多种实现如PHP,JavaScript,Java等各种语言开发包,程序实现简单。

安全性,OAuth是一个基于令牌的访问协议。用户通过令牌授权第三方应用访问其存储在服务提供者上的信息。其中没有涉及到用户账户、密码等信息。

开放性,OAuth对服务提供商和第三方开发者并没有限制,很多公司都提供了OAuth认证服务与OpenAPI。目前,开放平台支持包括第三方Web/Wap网站、PC桌面客户端应用、移动终端应用、各种浏览器插件应用以及各种开源建站系统的插件应用等来自第三方的各种类型应用。

1.2 OAuth协议认证流程

OAuth认证的基本思想[3]是第三方应用在需要访问用户开放平台上存储的数据时,会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授予第三方访问令牌,第三方客户端即可凭借该令牌,访问平台开放的应用接口。OAuth认证流程涉及以下四个角色[4]之间的交互。

资源拥有者:可以授权控制第三方应用访问开放平台中的受保护资源的网站用户,同时第三方应用的使用者。

第三方客户端:包含跨域访问开放平台中OpenAPI的客户端和OAuth认证授权的客户端,即需要获取授权和发送受保护资源请

收稿日期:2012-06-01
基金项目:宁夏大学科学研究基金项目(NE20120101-12)
作者简介:刘大红(1976-),女,陕西渭南人,同济大学研究生,中学一级教师,主要研究方向为软件工程、职业技术教育;刘明(1987-),男,山东泰安人,宁夏大学数学计算机学院研究生,主要研究方向为软件工程,网络安全。

求的第三方应用。

资源服务器:存储用户资源,响应第三方客户端的访问令牌和受保护资源请求的开放平台服务器。

授权服务器:能够成功验证资源拥有者和获取授权,并分发令牌的服务器。单独一个授权服务器可以为多个资源服务器分发令牌。OAuth认证流程如图1所示。

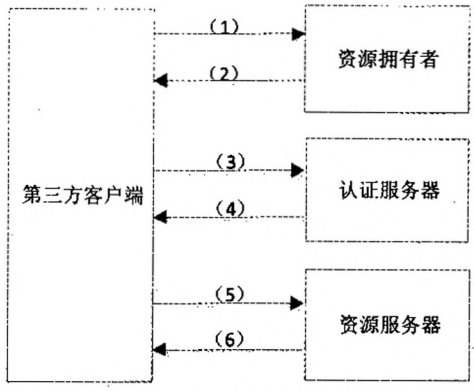

图1 OAuth认证流程图

(1)客户端向资源拥有者请求授权。授权请求直接发送给资源拥有者,或者间接的通过授权服务器发送请求;

(2)资源拥有者授权客户端,为客户端颁发一访问许可(Authorization Code);

(3)客户端提交自己的私有证书和(2)中得到的访问许可,向授权服务器请求访问令牌;

(4)授权服务器验证客户端的私有证书和访问许可的有效性,若验证有效,则向客户端发送一个包含许可作用域、有效时间等信息的访问令牌;

(5)客户端向资源服务器出示访问令牌,请求访问授权资源;

(6)资源服务器验证访问令牌,若有效,则客户端可访问资源服务器上受保护的资源[5]。

2 第三方应用与腾讯开放平台对接的设计及实现

2.1 腾讯社区开放平台OAuth认证分析

各社交网站开放平台认证流程基本一致,本文对腾讯社区开放平台进行分析开发。第三方应用的QQ登录接入流程如图2所示,图3描述了腾讯社区开放平台OAuth服务的认证过程。

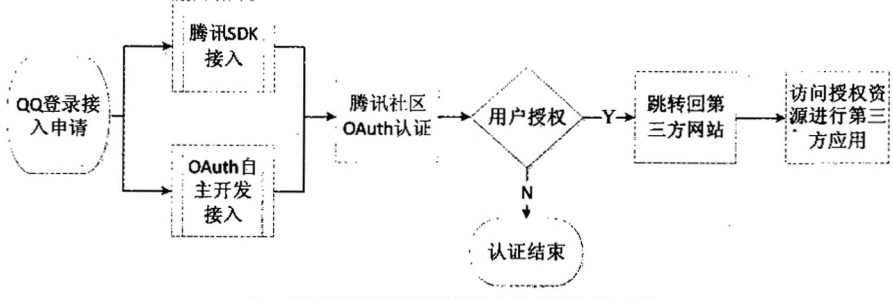

图2 腾讯开放平台第三方应用接入流程

第1步:申请QQ登录接入,获得appid与appkey;

第2步:使用腾讯开放平台提供的SDK包或者OAuth2.0协议,自主开发将appid与appkey嵌入网站程序,并填写QQ登录的回调地址,保证网站和openapi.qzone.qq.com的连接畅通;

第3步:向腾讯开放平台提交appid,获取未授权的Request Token;

第4步:请求QQ用户授权,若用户同意腾讯开放平台返回第三方授权的Request Token,用户不同意则返回登录页面;

第5步:使用授权后的Request Token向腾讯开放平台换取Access Token,跳转回第三方网站,完成认证;

第6步:根据access_token获得对应用户身份的openid;将Openid其与用户在网站上的原有账号进行绑定;

第7步:通过携带Acess Token访问OpenAPI,访问或修改用户授权的资源,如用户资料,日志,相册,说说等信息。

2.2 腾讯社区用户的BBS集成登录实现

本地BBS论坛基于JSP开发,因此选用腾讯的JS SDK进行二次开发,在页面顶部引入JS SDK库,在页面顶部引入JS SDK库,引入代码如下:

```
<script type="text/javascript" src="http://qzonestyle.gtimg.cn/qzone/openapi/qc_loader.js" data-appid="APPID" data-redirecturi="http://mengzhimeng.com" charset="utf-8"></script>
```

在本地BBS论坛登录页面中设置QQ登录按钮,调用上述引入SDK,

```
<span id="qq_login_btn"></span>
<script type="text/javascript">
```

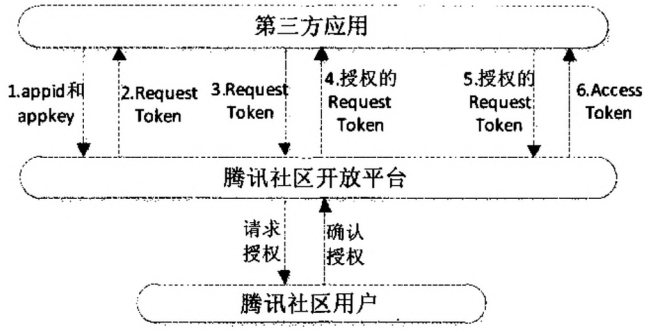

图3 腾讯开放平台OAuth认证流程

```
QC.Login({
    btnId:"qq_login_btn"    //插入按钮的节点id
})
```

当用户点击QQ登录图标是就会引导用户输入QQ号码和密码,跳转到腾讯开放平台,登陆成功后,第三方BBS会请求用户授权访问其受保护信息,效果如图4所示

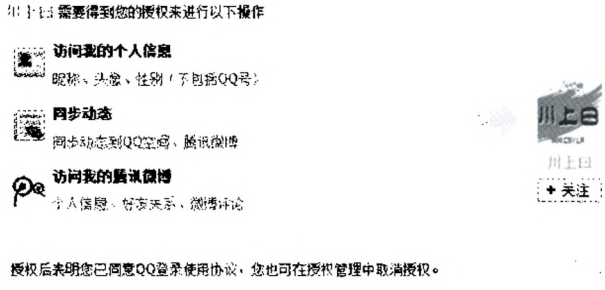

图4 腾讯社区OAuth认证授权页面

得到用户授权后,本地BBS就可以通过OpenAPI访问用户在腾讯服务器上的信息,调用get_user_info获取用户在QQ空间的个人资料,在不许用户操作,即可完善其在本地BBS中的个人基本信息,代码及注释如下:

```
<script type="text/javascript">
var paras = {};//用JS SDK调用OpenAPI
QC.api("get_user_info", paras)
    //指定接口访问成功的接收函数,s为成功返回Response对象
    .success(function(s){
        alert("获取用户信息成功！当前用户昵称为:"+s.data.nickname); //成功回调,通过s.data获取OpenAPI的返回数据
    })
    //指定接口访问失败的接收函数,f为失败返回Response对象
    .error(function(f){
                alert("获取用户信息失败！");
    })//失败回调
        .complete(function(c){alert("获取用户信息完成！");
    });//指定接口完成请求后的接收函数,c为完成请求返回Response对象
</script>
```

3 结束语

本文实现的第三方BBS站点与社交开放平台的对接登录,利于互联网企业共享用户群体优势,推广自身网站;同时减少了用户在多个平台登录的操作,实现互联网跨平台一站式社交体验。集成插件可以减少第三方开发者的代码编写,更加方便和快速的实现账号互联登录,将是开放平台OAuth认证服务的发展方向。

参考文献:

[1] RFC5849: The OAuth 1.0 Protocol[S].
[2] 刘镝,张智江,张尼.基于国内开放平台的Oauth认证框架研究[J].信息通信技术,2011(6):43-46.
[3] 张辉华,李炜.WDPF系统中认证授权流程的设计与实现[J].电信网技术,2010(11):89-93.
[4] 张卫全,胡志远.浅析作用于Web2_0安全防范的OpenID和OAuth机制[J].通信管理技术,2011,4(2):15-18.
[5] 时子庆,刘金兰,谭晓华.基于OAuth2_0的认证授权技术[J].计算机系统应用,2012,21(3):260-264.