利用OpenID和OAuth进行安全授权及风险防范的分析

刘 为 郝 梅

(武汉商业服务学院,湖北 武汉 430056)

摘 要:随着Web 2.0时代到来,不同厂商的Web应用出现了服务开放化和交叉化的趋势。在这种情况下,用户的个人授权信息是不同厂商建立联系的唯一纽带,我们需要一种安全的信息交互和授权机制来保护个人信息不泄露给第三方。本文着重分析了结合使用OpenID和OAuth两个开放协议进行用户信息安全授权的过程,并列举了可能出现的风险和防范方法。

关键词:Web应用,OpenID,OAuth,授权,风险

中图分类号:TP317 **文献标识码**:A **文章编号**:1009-2277(2011)05-0090-04

一、Web应用的发展现状

随着Web网络技术的飞速发展,网络应用层出不穷,以社交、分享为代表的web2.0应用已经融入了大众生活,成为网络发展的先锋,诸如国外的Facebook、Twitter、YouTube,国内的Sina微博、Tencent微博、QQ空间、人人网、360团购等,Web应用的开放化也成为服务商占领市场的一种方式。网络信息从分散的状态,向几个大型的网络应用中心聚拢;其他各种数据应用,为了得到更多用户访问量,都会向这些数据中心靠拢,请求用户数据,如Youku上的视频分享到Tencent微博,这些典型的应用不一定要服务商自己解决,服务商只需公开API给第三方应用,同时加上用户授权,第三方就可以代理用户实现数据交互。在这种信息交互中,第三方还可以获得用户的个人信息(已授权部分),并进行深度挖掘,实现了多方受益。

二、开放性Web应用平台的不安全因素

现在主流的应用平台,都实现了开放功能,即以API的形式,向第三方应用公开用户所授权的内容,这些第三方应用可以是网站,可以是专门开发的Web或桌面端应用程序,还可以是移动终端(手机、平板等)程序。信息的整合和获取变得更加简单,但是,相应的安全问题也很明显:

1、应用平台内的信息属于用户隐私,第三方在何种方式下能够合法的得到这些信息?

2、使用何种机制和技术,能够保障用户在授权过程中不透露或不被窃取个人信息,如用户名、银行账号、密码等。

3、应用平台如何审核与规范第三方应用,防止它们偷偷的收集用户个人信息,同时还需要防止不被授权的第三方应用非法取得权限。

基于以上问题,互联网上出现了两种开放应用协议,分别是OpenID和OAuth,其作用就是为开放平台提供规范、简洁、安全的通信、授权和管理机制。这两种协议已经得到了很多大型厂商的支持,如Yahoo,Facebook,Twitter,Microsoft,Google等,国内的sina,豆瓣,腾讯等都已开始应用这两项技术。

三、OpenID协议

OpenID是一种去中心化的身份认证,其不依赖一个集中的认证服务来工作,可以在任意支持该OpenID的网站完成认证工作。比如,用户在360的网站上注册成为会员,然后可以凭注册的用户名和密码,登录数十个与360合作的、支持该OpenID的团购网站,如美团网,拉手网等,而在这些团购网站上登录的效果,就犹如是已经在这些网站上注册了用户一样。这样的好处是,一次注册,可以在多个网

收稿日期:2011-07-29

作者简介:刘 为(1983-),武汉商业服务学院信息工程系教师。

郝 梅(1957-),女,武汉商业服务学院信息工程系主任,副教授。主要研究方向:图像处理、虚拟现实、数字媒体。

站上登陆,从而实现了跨域的单点登录(SSO)的功能,用户再无须进行重复的注册和登录。

OpenID 定义了三个身份和一个标识,如表 1 所示:

表 1 OpenID 身份和标识

名称	作用
用户(End User)	应用程序的使用者,想要向网站表明身份的人。
身份提供者(Identity Provider)	OpenID 的提供者,为每个用户提供一个 OpenID。
服务提供者(Relying Party)	支持使用 OpenID 登录的服务商
标识(Identifier)	最终用户用以标识其身份 URL 或 XRI。

OpenID 的工作流程如下:

1、用户(End User)需要使用服务提供者(Relying Party) 的服务时,要向其提供自己的标识(OpenID URL,可以在页面上输入,但一般是点击图标操作)。

2、服务提供者根据用户的 OpenID URL 与身份提供者(Identity Provider)进行通信,这里的通信有两种模式:一种是在后台进行,不提示用户;一种是使用访问服务提供者站点的同一个浏览器窗口与身份提供者服务器交互。其中第二种模式更为常用,接下来将以第二种模式分析。这一步结束后,服务提供者和身份提供者建立了通信。

3、服务提供者将用户引导到身份提供者的身份认证页面。

4、用户向身份提供者表明身份,并完成认证。

5、认证结束后,身份提供者将用户引导回服务提供者,同时返回的信息包含认证用户的结果判断,以及服务提供者需要的一些其它信息。

6、服务提供者判断返回信息的有效性,认证成功,用户即可使用相应的功能。

OpenID 跨域工作的方式,非常适合现在不同服务提供商之间的用户共享,一方面增加了服务提供商的潜在客户,另一方面也给用户提供了更好的登录体验。

四、OAuth 协议

OAuth 协议是一个开放的认证协议,其作用是为使用 API 的第三方提供安全、简单、标准的认证。简单地说,OAuth 允许用户授权第三方的应用访问他们存储在另外的服务提供者上的信息,而不需要将用户名和密码提供给第三方。比如人人网需要访问用户 QQ 好友列表的内容,用户需要授权给人人网,但是如果直接将用户的 QQ 号和密码发给人人网,很难保证其不记录下来,从而对用户产生安全威胁。OAuth 可以看作 OpenID 的一个补充,一般支持 OpenID 的服务都会使用到 OAuth。

OAuth 定义了 3 个身份,如表 2:

表 2 OAuth 的身份定义

名称	作用
用户(User)	资源拥有者,能够授权给服务提供者
服务提供者(Service Provider)	存储用户资源的中间者,在得到用户授权后,可以将资源提供给第三方
第三方服务者(Consumer)	独立的应用,需要访问用户存储在服务提供者的部分资源。

OAuth 大致工作方式如图 1:

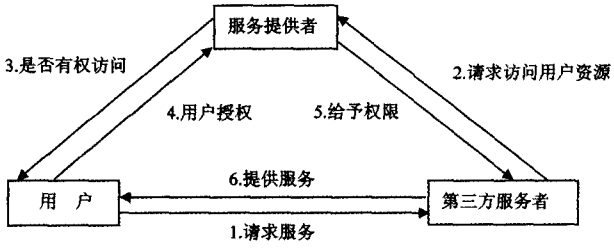

图 1 OAuth 工作流程图

其工作流程描述如下:

1、第三方服务者(Consumer)可以与不同的服务提供者(Service Provider)建立合作关系,每一个第三方的一个应用,都可以在服务提供者那里申请到唯一的 AppID(类似于登录名)或是公钥。

2、当用户向(User)第三方发出请求时,第三方提供一个 AppID 或者是公钥给服务提供方,服务提供方使用该公钥来确认第三方的身份,并与之建立通信。

3、第三方根据服务提供者发回的信息,将用户重定向到服务提供者网站所提供的登录页面。

4、用户登录后告诉服务提供者,该第三方访问他的保护资源是没问题的。

OAuth 认证过程中的一个关键技术叫做令牌(token),分为两种:

1、Request_token:一个临时的令牌,其作用是第三方在向服务提供者初次发出请求时,服务提供商返回的一个临时令牌。

2、Access_token:是第三方获得用户授权后,服务提供商提供给第三方的一个存取令牌,第三方凭此令牌与服务提供者进行通信,并可以访问用户资源。

OAuth 授权的过程中伴随着如下令牌的交换，其中 3 个 URL 是必须的，用于不同 token 的申请：

1、第三方向服务提供商的 Request _token URL 发起请求，获得未授权的临时令牌：Request _token。

2、第三方将先前获得的 Request _token，带上自身的信息（AppID 和用户要求等）发往服务提供商的 User_Authorization URL，并请求用户授权。授权后，再将授权 Request _token 返还给第三方。

3、第三方凭已授权的 Request _token 向服务提供商的 Access_token URL 发起请求，换取 Access_token，进而凭此令牌访问用户的资源。

从上面可以看出，OAuth 协议认证虽然也有用户登录的过程，但是，其登录始终是在服务提供者的页面登录，而并非在第三方的页面，从而保证了用户的登录名和密码不泄露给第三方。

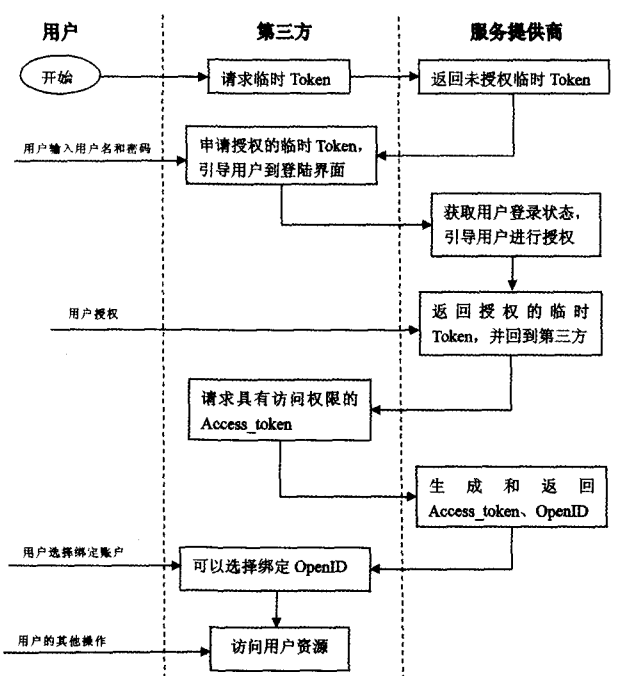

图 2 OpenID 和 OAuth 整合认证流程图

五、利用 OpenID 和 OAuth 进行认证的分析

通过上面的分析，OpenID 协议是服务提供者在与不同的第三方合作时，共享的一个唯一的用户 ID，而 OAuth 协议作用于当用户在第三方网站使用 OpenID 登录过程中，保证不将用户名、密码等敏感信息透露给第三方。两者结合起来使用，基本可以解决开放应用平台对第三方进行安全授权的问题。

接下来分析开放平台（即服务提供者，同时为 OpenID 提供者）结合使用 OpenID 和 OAuth 协议，对第三方应用进行安全认证的过程（流程图见图 2）：

1、开放平台并非对任何第三方应用都开放，为了管理它们，第三方应用首先应向开放平台申请一个独有的 AppID 和 AppKey（类似于用户名和密码），这一过程类似于用户注册成为网站的会员。完成注册后，第三方即受到了开放平台的认可，从而可以进行接下来的开发工作。

2、应用程序完成后，根据用户需求，第三方会向服务提供者请求访问用户资源，其方法是向网址 Request _token URL（一般也为 OpenID 的 URL）发送请求，请求包含 AppID 和 AppKey（之后的所有请求都需要这两个参数）。

3、服务提供者接受请求，验证 AppID 和 AppKey，之后返回未经授权的临时 Request _token 给第三方。

4、第三方得到未授权的临时 Request _token 后，向 User_Authorization URL 发出申请授权的 Request _token 的请求，在请求中加入 callback 地址。在请求发出后，第三方应按照要求将用户引导到服务提供商的登陆界面。

5、用户在登陆界面登陆后，完成授权工作，这时服务提供商将会生成授权的临时 Request _token，这其中包含一个唯一的 OpenID 值（该值并不安全，可能被篡改），并返回给第三方，同时将用户引导到第三方先前提交的 callback 地址上。

6、第三方收到授权的临时 Request _token 和 OpenID 值后，如果不再进一步需要访问用户的资源，而仅仅是完成登录的话，则到这一步即可。如果第三方想进一步访问用户的资源，则需要向服务提供者的 Access_token URL 申请具有访问权限的 Access_token，申请参数中需带上上面获得授权的 Request _token 值。

7、服务提供商根据请求，返回给第三方一个 Access_token 和一个 OpenID，这两个值是之后访问和修改用户数据所必须的参数。注意，这里返回的新的 OpenID 理论上是和第六步中的 OpenID 值相同，不过这一步返回的更加安全可靠，因为完全杜绝了用户篡改和伪造的可能性。同时，该 OpenID（也可以是 Access_token）也存在过期时间的问题，这需要服务提供商自行设置。

8、第三方获得了 Access_token 后可以访问和

修改用户的数据,这里的数据包含两部分,一是服务提供商提供了 API 的数据;二是还要验证用户为其数据单独设置的是何种权限:比如,第三方应用允许访问用户留言,但如果用户本身设置了留言不对外开放,则该应用还是无法访问。这种组合权限管理,需要服务提供商提前的设置,而不能依靠 OAuth 来设置权限的细节。

9、第三方获得了第 7 步得来的 OpenID 后,可以将其与用户在该第三方自身拥有的 ID 进行绑定。如果该用户之前没有该第三方应用的账户,第三方可以根据 OpenID 的信息为用户即时创建一个,并生成随机密码提供给用户,以便对该 OpenID 的管理。

六、依然存在的安全隐患

(一)"钓鱼"欺诈

采用 OpenID 和 OAuth 进行认证,依然无法防止"钓鱼"网站的欺诈。钓鱼网站可以伪装成与服务提供商合作的第三方,然后设置伪装的 OpenID 登陆框,诱使用户输入用户名和密码,从而窃取用户的信息。对于钓鱼网站的防范,主要是依靠用户预先安装的安全软件,以及有安全防护功能的浏览器。但更重要的是,对于大多数不了解钓鱼欺诈的用户来说,服务提供商可能需要安装浏览器插件或 ActiveX 插件进行即时的防护(几乎所有的网上银行都采用这种方式),比如当检测到用户输入了可能的敏感信息时,提醒用户查看当前网址是否为服务商的真实网址。

(二)地址伪造

在前面第五点分析的认证流程的第 6 步中,浏览器会返回一个 OpenID,但是这个 OpenID 的生成是在用户参与的情况下,即用户输入了用户名密码后的,这是个可以伪造的 OpenID,恶意攻击者可以对网站进行虚假登录。同时,如果攻击者获得了 AppID 和 AppKey,也可以伪造签名,从而生成伪造的 OpenID。防范这种风险的方法是,在使用返回的 OpenID 之前,必须要对其进行效验,确保和服务端的 OpenID 相同,或是使用上面第五点分析的认证流程中的第 7 步返回的 OpenID,因为这一步返回的 ID 是由第三方在后台与服务提供商进行的通信而生成的,这一过程中并没有用户的参与。

[参考文献]

[1] 刘敏,吕先竞,宋玉忠. 基于 OpenID 的分布式认证系统的设计与实现[J]. 现代情报, 2008 (06).

[2] 张明西,刘晖. OpenID 标准化认证机制的研究与应用[J]. 计算机应用与软件, 2010 (07).

[3] 阮高峰,徐晓东. OpenID 分布式身份认证系统及其教育应用展望[J]. 中国电化教育, 2008 (11).

[4] 许彤,雷体南. OpenID 与 OAuth 技术组合应用于教学资源库建设[J]. 软件导刊(教育技术),2009(10).

[5] 张卫全,胡志远. 浅析作用于 Web2_0 安全防范的 OpenID 和 OAuth 机制[J]. 通信管理与技术,2011(02).

[6] 夏晔, 钱松荣. OpenID 身份认证系统的认证等级模型研究[J]. 微型电脑应用,2011(04).

责任编校:邓小妮

The Analysis of the Use of OpenID and OAuth for Authorized Security and Risk Prevention

LIU Wei HAO Mei

(Wuhan commercial service college, WuHan, Hubei, 430056, China)

Abstract: With the Web 2.0 era, there is a trend of opening up of services and digitalizing cross by Web applications from different vendors. In this case, personal information of users is authorized by different manufacturers which is the only contact link built by them. A safe information interaction and authorization mechanism are needed to protect personal information without leaking to the third party. This paper focuses on analyzing the process of users information security authorized by combining two open protocols OpenID and OAuth, and listing the possible risks and prevention methods.

Key words: Web application; OpenID; OAuth; authorized; risk.