浅析作用于Web2.0安全防范的OpenID和OAuth机制

张卫全，胡志远
（上海贝尔股份有限公司，上海 201206）

摘 要：分析了Web2.0的安全漏洞和安全威胁，介绍了两个开放式的身份认证协议即OpenID和OAuth，并建议结合OpenID和OAuth来保护Web2.0中的网络资源，防止网络资源遭到有意或无意的滥用。

关键词：安全机制；Web2.0；OpenID；OAuth；认证
中图分类号：TP393.08 文献标识码：B 文章编号：1672-6200(2011)02-0015-04

1 引言

Facebook、Twitter、YouTube、Wikipedia、开心网、人人网等Web2.0网站正在逐步为用户创建一个服务完备的网络社会，启动了网络生活和现实生活趋同的过程。这些社交网络是用于人际关系的社会服务平台，方便人们参与一系列的社会化活动，如商务、教育、购物、理财等，使人们的生活更加丰富多彩。然而，正是由于社会网络服务于用户人际关系的原因，有很多途径容易泄漏用户的私密信息，同时也为恶意软件攻击网络提供了多个渠道。2010年10月18日，华尔街日报报道了Facebook许多热门应用软件一直都在泄漏用户的私密信息(如身份、好友名单)，把这些信息发送给数十家广告和互联网追踪公司。Websense公司分析报告指出，从2009至2010年，恶意网站的数量增加了111.4%；79.9%的合法网站受到了恶意代码的攻击，相比2008至2009年同期增长了3%。

幸运的是，可以使用一些安全措施来降低以上所述的泄漏私密信息、恶意代码攻击等风险。先进的认证和授权协议可以集成到社交网站和应用程序中，用户只需要使用一套认证凭证(如一个用户名/密码)，就可以安全地在社交网站上活动，并共享用户信息。目前有两个主要的Web2.0安全机制，即OpenID(Open Identity)和OAuth(Open Authentication)。

下面就介绍Web2.0的这两个安全机制—OpenID和OAuth，以及结合使用这两个安全机制保护Web2.0网络资源的问题。

2 Web2.0的安全威胁

Web2.0的发展为商务和个人社交活动创造了很多网络上的机会。无论用户处于何时何地，Web2.0都能为用户提供开放的资源，让其获取信息。Web2.0还允许浏览器访问应用程序让用户获得更高效的社交网络互动的资源，这在以前无法想象，因为在社交网络出现前，应用程序只能由台式机访问。

然而，Web2.0迅速发展的同时，也出现了许多安全隐患。下面分析Web2.0的安全漏洞和安全威胁。

Web2.0的主要安全漏洞有：

(1)一个重要的漏洞是Web2.0环境中授权访问机制不健全，这主要是因为很难在快速开发应用的自由与提供适当安全保护之间找到平衡点；

(2)给用户提供更多的机会去创造网络内容，同样也给攻击者注入恶意代码提供了更多的可能，很短的开发周期，加上许多

程序员没有或很少经过安全培训，就更加扩大了安全漏洞出现的可能；

(3)信用危机泛滥，凭空给不良之徒以千载难逢的机会，使他们为发布欺诈信息(如股票价格欺诈信息)有了可乘之机；

(4)留言板、博客等社交网站也是泄漏信息的一个途径，所以，Web2.0给许多企业带来方便与好处的同时，也给企业造成了丢失重要数据的困难；

(5)Web2.0环境中用户随时产生的大量信息，即使Web安全处理方案高效，也很难实时深度地分类、分析解决这些内容里暗藏的问题。

以上Web2.0安全漏洞带来了如下安全威胁：

(1)身份信息丢失；

(2)个人信息泄漏；

(3)恶意软件、间谍软件使财产流失；

(4)虚假和误导信息的传播；

(5)滥用资源，如盗打电话。

因此，除了传统的Web安全机制如URL过滤以外，Web 2.0的安全保护需要新一代的先进安全机制。为了系统地减小Web2.0的安全风险，除了先进的安全技术，还需要考虑更多各方面的因素，如人员管理、流程和技术、用户安全意识、政府政策、安全开发和部署等。

多种安全机制多管齐下，就可以降低Web2.0的安全风险。目前有两个主要的Web2.0安全机制是：OpenID和OAuth。一些大型的社交网络如Facebook已在使用，为用户提供了隐私保护和网络资源保护。

3 OpenID

OpenID是一个开放的身份认证协议，它描述了用户如何以分布式的方式认证身份。这样，服务提供商只需要关注自己的业务体系本身，而不用再重复考虑认证机制，同样也使用户可以集中地统一管理自己的身份信息，如OpenID URL。

协议OpenID不依赖于一个集中的认证中心来认证用户的身份。此外，无论是业务还是OpenID标准，都不需要强制一种特定的认证机制来认证用户。因此，用户的认证机制可以有多种，通用的认证方式(如用户名/密码)或其他新颖的认证方式(如智能卡或生物识别技术)都行。

OpenID定义了如下3个角色：

(1)用户(User)：终端用户，能使用程序(如Web客户端)访问OpenID提供商或业务提供商；

(2)业务提供商(Service Providers，即OpenID支持方Relying Parties)：能支持用户以OpenID身份登录网站，如LiveJournal、WikiSpaces等；

(3)OpenID提供商(OpenID Providers，即身份认证协议提供商Identity Provider)：提供OpenID业务，如注册OpenID身份、OpenID URL或OpenID XRI、存储用户OpenID身份、及提供OpenID的身份认证，如AOL、Yahoo!、Verisign等。

OpenID工作流程如图1所示。

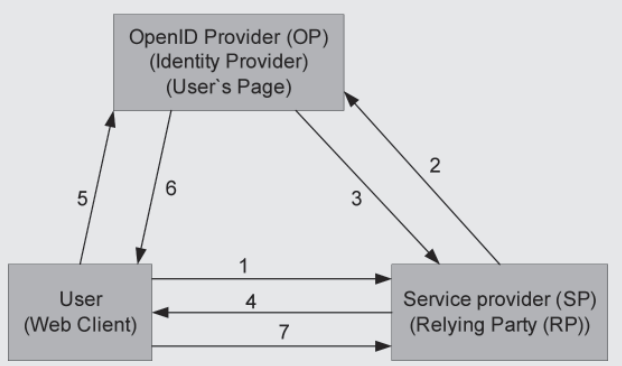

图1 OpenID工作流程

OpenID工作流程概述如下：

(1)用户(User)登录业务提供商(Service Provider)网站时，在业务提供商的页面上输入OpenID身份，即OpenID URL或OpenID XRI；

(2)业务提供商根据用户提供的OpenID身份信息与OpenID提供商通信；

(3)初始化业务提供商和OpenID提供商之间通信；

(4)业务提供商将用户引向OpenID提供商认证身份；

(5)用户提供自己的认证凭证给OpenID提供商，并认证；

(6)认证结束后，OpenID提供商将用户引向业务提供商，送去的消息包含认证用户后的断言和业务提供商要求的相关属性；

(7)业务提供商验证断言与相关属性的有效性，验证成功，用户就能访问业务提供商提供的业务。

OpenID支持单点登录(SSO，Single Sign-On)，即用户最初访问网站的一次身份认证，就能访问所有授权的网站。OpenID还能提供跨域认证，即使是不同的多个网站用户也不需要注册多个账户，从而提高了用户的工作效率，降低管理费用，并提高网络的安全性。然而，OpenID也有一些弱点，例如容易受到网络钓鱼攻击。

一些电信运营商计划为移动互联网部署OpenID服务。一些电信设备商正在研究如何将OpenID用到现有网络，为电信运营商使用OpenID服务做准备。由于OpenID协议本身没有指定任

何用户认证机制，因此一些标准组织如3GPP已制定了将现有的网络接入安全认证机制用到OpenID，为用户提供身份认证，如3GPP TR33.924。

4 OAuth

OAuth是一个开放的认证协议，允许用户在不泄露用户名/密码的情况下，和其他网站共享存储在另一个网站上的个人资源(照片、视频、通信录等)。例如，一个支持OAuth的照片共享网站，允许用户使用第三方打印网站在不需要获得用户账户/密码的情况下，访问和打印用户的私人照片。

OAuth是一种服务，不同于OpenID，但与OpenID相辅相成。OAuth是为了让用户授权一个应用程序去访问用户的信息，如他的网上相册或通信录及好友列表。这可以让用户很容易与多个网站共享信息，如在线相册。

IETF目前正在起草OAuth2.0协议，同时Twitter、Facebook、Google、AOL几个大型网站也在开发和部署OAuth2.0协议，为用户信息和网络资源提供安全保护。

OAuth2.0定义了如下4个角色:

(1)资源所有者: 一个实体，能授权一个应用(即客户端)访问受保护的资源;

(2)客户端: 一个应用程序，能获得授权并请求访问受保护的资源;

(3)资源服务器: 一个服务器，能接收受保护资源的访问请求，并能应答请求的受保护的资源;

(4)授权服务器: 一个服务器，能成功认证资源所有者及获得资源所有者的授权，认证成功及获得授权后能发布访问令牌。它可能与资源服务器合设，也可能是一个独立的网络设备。

OAuth2.0工作流程如图2所示。

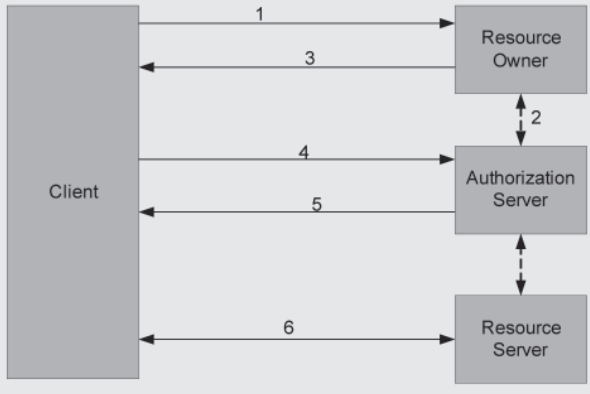

图2　OAuth工作流程

OAuth2.0的工作流程简述如下:

(1)客户端想要访问受资源所有者控制的网络资源，但客户端并不知道资源所有者的认证凭证。客户端需要在授权服务器注册，以便获取客户端的认证凭据(如client_id，client_secret);

(2)客户端请求资源所有者授权，访问用户的网络资源;

(3)资源所有者在授权客户端访问前，资源所有者需要通过授权服务器的认证;

(4)资源所有者认证成功后，客户端接收到一个访问资源授权凭证，授权凭证代表资源所有者允许客户端访问网络资源;

(5)客户端向认证服务器请求访问令牌，请求消息包含用于认证客户端的认证凭证和访问资源的授权凭证;

(6)授权服务器根据客户端的认证凭证认证客户端，并验证资源访问授权凭证的有效性，如果都成功，则向客户端发布一个访问令牌;

(7)客户端向资源服务器请求访问受保护的资源，请求包含一个访问令牌。资源服务器验证访问令牌的有效性，如果有效，则客户端能访问资源服务器上受保护的资源。

OAuth是一个令牌的协议，能用于Web2.0中授权第三方安全访问网络资源。然而在OAuth Core1.0第6章令牌申请审批流程中，可能会遭到会话攻击(如session fixation attack)。访问令牌有可能过期或失效，所以需要有访问令牌更新机制。OAuth1.0所遇到的攻击，在OAuth2.0都考虑到了，有所防备。

一些电信运营商已认可OAuth能确保第三方应用安全访问电信网络资源，而且GSMA RCS已经明确要求使用OAuth2.0来保证网络资源的授权访问。

5 在Web2.0中结合使用OpenID和OAuth

OpenID提供的服务是不同的消费者(如第三方应用程序)共享用户的一个单一身份信息。OAuth提供的服务是不同消费者可以分享用户的网络资源而不用知道用户的认证凭证(用户名/密码)。在Web2.0中，OpenID和OAuth可以很好地协同工作，以便保护用户网络资源。

为了增加利润，电信运营商希望开放底层网络资源给第三方应用。但如果没有安全机制，网络资源可能会遭受到有意无意的滥用或攻击。结合使用OpenID和OAuth，能有效地减少攻击或滥用电信网络资源的可能性。

图3所示Web2.0中结合使用OpenID和OAuth来保护网络资源的工作流程简述如下:

(1)作为客户端的应用和内容提供商在不知道资源所有者认证凭证的情况下想访问该资源所有者所控制的网络资源。客户端

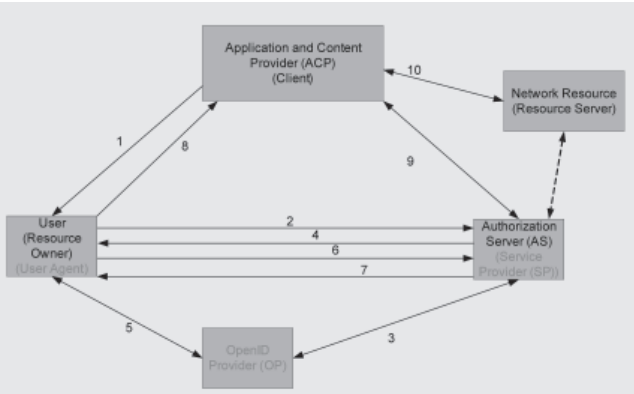

图3 Web2.0中结合使用OpenID和OAuth来保护网络资源

可能需要在授权服务器处进行注册以便获取客户端的认证凭据(如client_id，client_secret等)，OpenID提供商有可能和授权服务器合设，本文描述的是授权服务器和业务提供商合设的场景；

(2)客户端请求资源所有者授权其访问该用户的网络资源；

(3)资源所有者请求授权服务器授权该客户端去访问其网络资源，并提供其相应地URI、断言(如果有)和她/他的属性给客户端(如果需要)。如果资源所有者的断言有效，则直接进入第7步，否则，具有授权功能的服务提供商要求按照步骤3～6来对该资源所有者进行身份认证；

(4)具有授权功能的服务提供商根据所提供的URI与OpenID提供商进行通信，并初始化具有授权功能的业务提供商和OpenID提供商之间通信；

(5)具有授权功能的服务提供商重定向资源所有者到OpenID提供商那进行身份认证；

(6)资源所有者使用其认证凭证(如密码)登录OpenID提供商，认证成功后，OpenID提供商将该资源所有者重定向到具有授权功能的业务提供商，该消息中包含资源所有者的断言和其相应地属性(如果需要)；

(7)资源所有者将其断言和她/他的属性提交给具有授权功能的业务提供商；

(8)具有授权功能的业务提供商发布资源访问授权凭证给用户代理；

(9)用户代理将资源访问授权凭证转发给客户端；

(10)客户端向具有授权功能的业务提供商请求访问令牌，该请求中包含客户端的认证凭证和资源访问授权凭证。具有授权功能的业务提供商根据客户端的认证凭证认证客户并验证资源访问授权凭证的有效性，验证都成功后，具有授权功能的业务提供商将发布一个访问令牌给客户端；

(11)客户端向网络资源服务器请求访问受保护的网络资源，该请求中包含访问令牌，网络资源服务器验证客户端提供的访问令牌的有效性，如果有效则客户端可以访问资源服务器处受保护的资源。

通过结合OpenID和OAuth，确保只有经过资源所有者授权且经过身份认证的应用才可以访问所保护的网络资源，从而可以减少网络资源滥用的风险。

作者简介：

张卫全，男，硕士，先后从事交换、传输等设备的现场测试以及GSM产品的研发等工作。

胡志远，女，博士，现主要从事通信安全的研发和标准化工作。

收稿日期：2011－03－14

·资讯·

WLAN芯片组今年出货量将超7亿个

由于Wi-Fi成为多种电子产品中的必备功能，某公司预计无线局域网(WLAN)芯片组市场在2011年将扩大一倍，WLAN芯片组出货量将达到7.389亿个。比2010年的3.668亿个大增101.5%，这些芯片组用于各类电子产品，使消费者能够共享内容。预计2012年其出货量将超过10亿个。据了解，WLAN芯片组具有独立与嵌入两种形式。对于独立WLAN芯片组，2010年Wi-Fi嵌入设备的总体出货量达3.66亿个，比2009年剧增135%。而嵌入解决方案，提供连接性的WLAN芯片组已渗透到多种电子产品，包括笔记本电脑、手机、平板电脑、高清电视等。业内人士认为，随着Wi-Fi逐渐成为无数设备的标准无线网络接口，包括该技术内在的轻松互联能力将为更多的消费电子设备创造条件，使之实现无缝连接和联网。

欧盟呼吁加速部署卫星移动服务

欧盟委员会数字化议程副主席对21个欧盟成员国发出紧急呼吁，希望他们能在短时间内推出必要的法律举措，以实现卫星移动服务的泛欧部署。卫星移动服务是一种新型的无线通信服务，可以用于高速互联网、移动电视和无线电或应急通信，其优势在于可以提供泛欧覆盖。“欧洲数字化议程”着重强调了无线宽带(卫星和地面)对提高宽带覆盖率(包括偏远和农村地区)所起到的关键作用。