OpenID与OAuth融合认证中令牌安全提升方法*

张 宇 胡 健

(中国科学院声学研究所高性能网络实验室 北京 100190)

摘要:移动互联网、物联网的资源交换共享。需要一种开放的身份认证与授权机制。OpenID与OAuth融合能够满足需求,也被很多互联网公司的业务平台所采用。但令牌存放位置可导致令牌泄露,而融合协议频繁的重定向则增大了令牌泄露风险。本文通过对协议建立形式化表达模型,用软件工具分析了协议安全性,证明了令牌通过Cookie存放是问题所在。通过调整融合认证的体系结构,在认证过程参与的实体上应用本地多级信任缓存,可以减少30%~50%的认证信令,提高了令牌的安全性。针对令牌攻击及相关的安全建议,进行了改进前后的对比验证,实验结果表明该方法可有效抵御针对令牌的网路攻击,提升平台的安全性。

关键词:物联网,资源共享,认证,令牌,OpenID协议,OAuth协议

A Token Security Improvement Method for OpenID and OAuth Collaborative Authentication

ZHANG Yu, HU Jian

(Institute of Acoustics, China Academy of Sciences, Beijing, 100190, China)

Abstract: An open identity authentication framework is needed for resource sharing in mobile internet and/or Web of Things (WoT). The OpenID and OAuth collaborative framework meets the basic requirement and is adopt by some Internet companies. But the collaborative frame work could have the risk of Token Leaking. In this paper, we adjust the authentication framework and apply a multi-entity cache based method. These methods reduce the authentication process lower to 30%~50% and increase the Token security. The experiment shows that this framework can defend the token theft well thus promote the security level of the authentication framework.

Keywords: WoT, Resource sharing, Authentication, Token, OpenID, OAuth

1 概述

移动互联网、物联网发展过程中会产生海量数据。由于数据权属和缺乏数据交换共享机制,目前整体上存在数据资源孤岛的问题,制约了数据价值的挖掘和利用。因此实现网络资源共享是当前物联网研究中一个热点。

目前基于资源共享的身份认证应用最广泛的协议有OpenID[1]与OAuth[2]两种。OpenID是一种单点登录协议,用户用一个用户名及密码就可以访问所有支持该协议的Web站点。OAuth允许第三方客户端在无需提供用户密钥的前提下从Web服务中获取受保护资源。OpenID与OAuth融合的身份认证机制综合这两个协议的特点,不仅能够实现单点登录、资源开放,而且能够让资源所有者细粒度地控制对资源的授权,能

本文于2014-10-10收到。
*基金项目:国家重大专项(2011ZX03005-006)。

够知道是谁访问了哪些资源以及访问量。

为了提高认证协议的效率,通常选择将令牌存储于依赖方 RP(Relying Party)的 cookie 域中。研究得知:①29% 的 RPs 自动设置 cookie。②17% 的 RPs 将令牌作为静态参数传给注册节点。③7% 应用令牌透过 APIs 访问用户注册信息[3]。这种为了降低认证复杂度而采取的方法,会造成令牌泄露风险。

针对这个令牌安全问题,本文首先进行定量、定性分析,给出导致融合协议令牌泄露的原因。进而提出一种本地的多级信任缓存方法,试图解决这个问题。通过实验验证,本方法提高了数据平台抵御攻击的能力。

2 相关工作

文献[4]提出基于委托许可的认证授权方案。这是探索 OAuth 协议与已有统一管理密钥体系相结合的初步试探。然而该方法存在令牌访问权限不可控等诸多问题,并未得到广泛应用[5]。

文献[6-8]提出综合 OpenID 与 OAuth 协议的特点,建立一种融合的身份认证机制。该机制虽然整体上符合资源共享、身份认证的需求,但对协议本身的安全性问题,特别是令牌泄露风险,并未涉及。协议融合后对此类风险产生怎样影响,相关文献并未进行深入分析。

Google 提出了基于 OpenID 与 OAuth 的扩展协议[6]。协议将 OpenID 的认证请求与 OAuth 申请令牌许可相结合,并要求 OpneID 提供者 OP(OpenID Provider)与 OAuth 服务提供商为统一服务端,RP 与 OAuth 消费者为同一服务端。这种设计使得融合协议具有一定局限性,不能解决当 RP 与 OAuth 消费者不同时的认证需求。

文献[7]中 IBM 团队提出 OpenID 与 OAuth 在 SaaS(软件即服务)中协同服务。该应用为身份管理体系建立服务装载平台(SDP)。在服务平台中设置两个重要组成部分:①OpenID RP 组件。②OAuth 提供者或消费者组件。该协议使得服务提供商之间可以相互调用,与文献[6]方法相比通用性得到提升。但该体系中所有服务都需要与 SDP 进行交互,这造成每次产生一个资源请求,资源申请流程都被完整执行两次,这使得 SDP 成为系统瓶颈。

文献[8]在文献[7]的研究基础上做出改进,取消 SDP 的同时实现共享程序的自由交互。该认证机制虽然解决了 SDP 瓶颈问题,但是资源访问的申请流程与文献[7]相比有所增加,资源交互复杂性加大,协议融合带来的结构性安全风险未知。

3 融合协议令牌安全性分析

文献[9]按照谓词分析方法对 OAuth 协议作了形式化表达。其中定义如下角色及映射关系:

R(x):x 代表资源服务器(Resource Server)

O(x):x 代表资源拥有者(Resource Owner)

C(x):x 代表用户(client)

A(x):x 代表授权服务器(Authorization Server)

定义如下关系类型:

Owns 关系:表示协议中一个成分(principal)对一个值拥有管辖权。例:

$$\forall x(O(x)\rightarrow(\exists ROC(y)\cap owns(x,y))$$

表示一个资源拥有者拥有自己的认证密钥。

Draws 关系:代表一个 principal 从协议执行时就持有一个值 y。例:

$$\forall x(A(x)\rightarrow(\forall yROC(y)\cap draws(x,y))$$

表示所有授权服务器都有一份认证密钥拷贝。

Computes 关系:一个成分用已存在于本身的另一个值来计算一个值。例:

$$\forall x(C(x)\rightarrow(\exists yATR(y)\cap Computes(x,y))$$

表示用户可以计算已经传递了其它信息的用户令牌申请消息。

Learns 关系:协议中一个 principal 在与其它 principal 交互时获取的值。例:

$$\exists x\exists y(A(x)\cap C(y)MSG(y,x)\rightarrow learn(x,y))$$

表示任何时候当一个消息从用户传递给授权服务器时服务器都能从用户处得知消息信息。

通过上述角色及关系对 OAuth 协议建立协议模型:

```
sig Authorization extends Principal{
learns1: RedirectionURI,
learns2: ClientPassword,
learns3: AuthorizationGrant,
learns4: PermissionResponse,
draws1: ResourceOwnerCredentials,
draws2: PermissionRequest,
draws3: AuthorizationCode,
draws4: ErrorResponse,}
```

图 1 为根据上述关系利用 Alloy 分析器构建的协议反例模型图。对图 1 分析可得,协议的安全风险主要在于 URI 的重定向导致令牌的泄露风险。而这种形式化的分析结果也说明了令牌存储的安全性问题是身份认证协议存在的关键性隐患。

选取文献[3,10]中介绍的攻击模型,通过对主流的认证授权服务平台进行验证性研究,分析该风险的普遍性。图 2 为文献[3]中样本受多种攻击的风险比率,由于每个样本可受到多种攻击,攻击有重叠部分,因此总体比率在图中大于 100%。

由图 2 可知,在五个攻击样本中,约 70% 以上为针对令牌(Access Token)的攻击,其中 RP 抵御令牌盗取与 HTTP 伪装能力最弱。

通过以上分析得知,OpenID 与 OAuth 融合协议的安全隐患主要来自几个方面:①URI 重定向带来密钥泄露风险;②令牌存放的安全性问题;③令牌的权限控制问题。

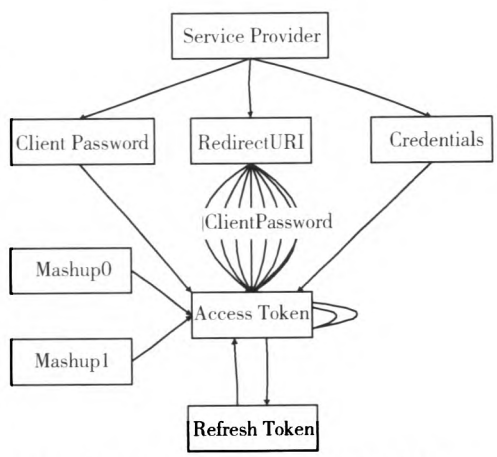

图 1　基于 Alloy 分析器构建的反例模型图

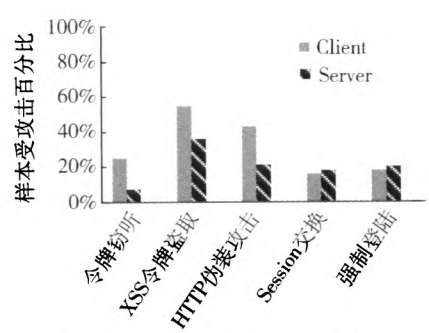

图 2　客户端与服务端受到各类攻击危险的百分比

4　令牌安全性改进

4.1　体系结构

将资源共享平台作为 OpenID 授权服务器及 OAuth 用户授权凭证的授权服务器。服务(Service A 、Service B)既可以作为 OAuth 协议的客户端,也可以作为资源提供商。

图 3 为融合认证协议体系结构。将资源共享平台作为 OpenID 授权服务器及 OAuth 用户授权凭证的授权服务器。服务(Service A, Service B)既可作为 OAuth 协议的客户端也可以作为资源提供商。

这种结构的改进主要有:

(1)OpenID 模块与 OAuth 模块共同处于平台中。这有助于对平台提供的资源及资源提供商提供的资源进行分级处理,避免各模块之间不必要的网络信令交换。

(2)用户的 OpenID 作为平台认证凭证进行 OAuth 两步验证的第一步,可以简化融合协议复杂度,减少信令泄露风险。

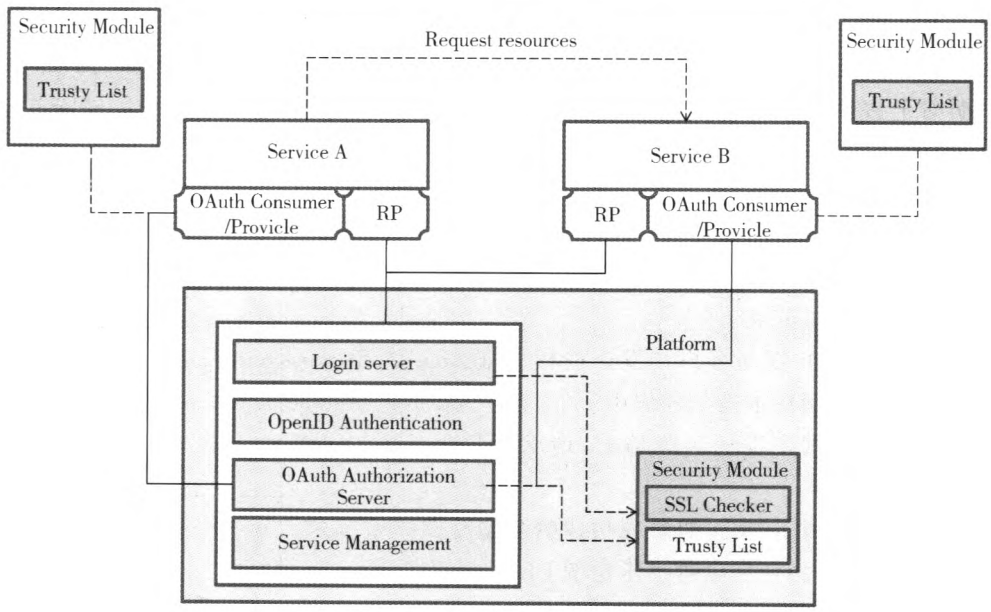

图 3 融合认证协议体系结构

4.2 多级本地缓存结构

在平台与资源提供商多级建立本地信任表对认证授权过程中的信息进行缓存。信任表结构如表 1、表 2 所示。

表 1 授权认证平台信任表

字段	用户 ID	用户授权凭证	生存周期	预留
格式	Varchar(255)	Char(128)	DATATIME	Void

表 2 资源提供商信任列表

字段	用户 ID	授权令牌	资源 URI	生存周期	预留
格式	VARCHAR(255)	CHAR	VARCHAR	DATATIME	Void

该缓存信任表可避免令牌存于 cookie 中而遭到网络攻击;通过建立信任关系,对于重复的资源请求可避免过多的重定向行为。在信任表中采用令牌与 URI 配对原则,可明确令牌访问权限。同时在申请令牌时向用户询问令牌生命周期,可确保令牌在周期内合法原则;在 RP 端,改进后的协议模型在登录及注册时增加了 SSL 保护,并针对网络钓鱼攻击[11]做出了改进。

根据文献[3,5,12]中提出的针对网络攻击的改进建议,表 3 显示了采用信任缓存前后,网络安全性的对比。

从表 3 中可以看出,采用信任缓存后实现了多项上述文献中的提高网络安全性的建议。

表 3 融合认证协议改进前后对比表

	建议	改进前	改进后
IdP	强化注册与登录过程	N	Y
	重定向页面的验证	N	N
	令牌刷新机制	N	N
	强化单点登录授权	N	Y
	阻止令牌存于 cookie	N	Y
	征求用户许可	N	Y
	明确令牌权限	N	Y
RP	登录时 SSL 保护	N	Y
	上下文绑定验证	N	Y
	登录域独立管理	N	N

注:N - 未实现;Y - 实现

5 功能性能分析

资源共享认证流程如图 4。以下为具体的访问流程:

(1)客户端向资源提供商请求资源,如果客户端存有之前成功申请的访问令牌(access token),则一并将其发送给资源提供商。

(2)资源提供商与平台进行通信。如果客户端提供了访问令牌,则资源提供商通过本地的信任列表(trusty list)检查访问令牌有效性。如果有效,则认为客户端在平台的信任表中也存储了客户信用凭证,并且有效,跳转至步骤(10)。

(3)如果资源提供商信任表中无该令牌或者虽然存在,但令牌已经过期,则重定向至客户端。

(4)客户端向平台请求授权凭证,平台通过信任表检查客户端凭证,如存在且有效,则转至步骤(7),发送该授权凭证。否则转至步骤(5)。

(5)平台重定向至用户。

(6)用户发送用户密钥(OpenID/密码),验证客户信用。

(7)如果平台验证成功,则向客户端发送授权凭证,并同时将客户信用凭证存储在本地信任表中。

(8)客户端向资源提供商发送令牌请求,请求信息中带有授权凭证。

(9)资源提供商验证授权凭证,如果成功,则向客户端发送访问令牌,客户端利用访问令牌请求资源。

(10)验证访问令牌,如果有效则发送受保护的资源,同时令牌信息存储在资源提供商本地信任表中。

从这个流程中可以看出,通过建立一种逐级缓存机制,在提高安全性的同时对用户进行逐级认证优化处理,可有效地缩短访问流程(见图 4)。

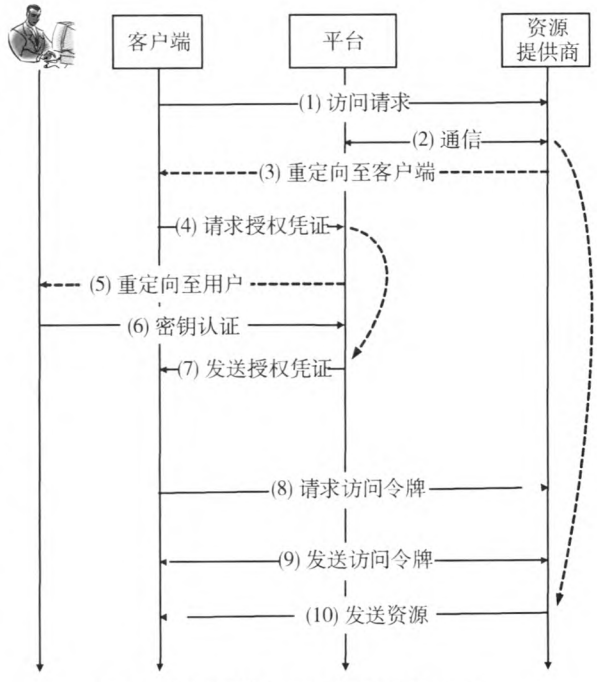

图 4　资源提供商授权资源访问流程

(1)用户本地存有访问令牌,资源提供商本地信任列表访问令牌有效。在该情况下只需 30% 流程即可实现资源访问。

(2)用户无令牌或者令牌无效,但平台处存有用户认证信息。该情况下可减少一半左右的访问流程。

为了验证改进后的认证模型对于令牌安全性的改进,选取文献[3]中针对令牌的攻击模型,对改进前后进行验证,验证如表 4 所示,对比改进后的措施可有效抵抗针对令牌的攻击。

表 4　改进前后抵抗攻击对比表

	改进前	改进后
令牌窃听	N	Y
XSS 令牌盗取	N	Y
HTTP 伪装攻击	N	Y
Session 交换	N	N
强制登陆	N	N

注:N - 未实现;Y - 实现

6　结束语

目前融合 OpenID 与 OAuth 的身份认证协议存在令牌泄露的安全风险。本文通过分析,找出风险产生的原因,进而提出基于本地多级信任缓存的方法,构建改进的融合认证体系。通过实验证明此方法提高了安全性。本质上说,该方法是为各级信任关系建立统一管理机制,满足安全性与实用性需求。

参　考　文　献

[1] Hyun - kyung Oh, Seung - hunJin. The SecurityLimitations of SSO in OpenID. [C]. In:10th International Conference on Advanced Communication Technology, 2008. ICACT 2008 Pages:1608 - 1611

[2] Leiba,B. Oauth Web Authorization Protocol. [J]. Internet Computing IEEE. 2012,10. 1109/MIC. 2012. 11. Page(s):74 - 77

[3] San - Tsai Sun and Konstantin Beznosov. The devil is in the (implementation) details: An empirical analysis of OAuth SSO systems. In Proceedings of ACM Conference on Computer and Communications Security (CCS'12), October 2012. Page(s):378 - 390

[4] Hasan R, Conlan R, Slesinsky B,et al. Please permit me: stateless delegated authorization in mashups. [C]. In:Annual computer security applications conference (ACSAC); 2008,10. 1109/ACSAC. 2008. 24 Page(s):173 - 182

[5] Noureddine,M. Bashroush,R. Aprovisioning model towards OAuth2.0 performance optimization. [C]. IEEE 10th Internation Con-

ference on Cybernetic Intelligent Systems(CIS). 2011. 10. 1109/ CIS. 2011. 6169138. Page(s):76 - 80

[6] OpenID OAuth Extension Website. [OL]Last accessed in December,2009. http://step2. googlecode. com/svn/spec/openid_oauth_extension/lastest/openid_oauth_extension. html.

[7] Wang Bin,Huang Heyuan,Liu Xiaoxi,et al. Open Identity Management Framework for SaaS Ecosystem. [C]. IEEE International Conference on e - Business Engineering, 2009. 10. 1109 /ICEBE. 2009. 82. Page(s):512 - 517

[8] DingChu,Qing Liao,Jingling Zhao. Open identity management framework for mashup[C]. IEEE 2nd Symposium on Web Society (SWS),2010,10. 1109/SWS. 2010. 5607421,Page(s):378 - 382

[9] Pai, S.; Sharma, Y. ; Kumar, S. ; Pai, R. M. ; Singh, S.. Formal Verification of OAuth 2. 0 Using Alloy Framework[J]. 2011 International Conference on Communication Systems and Network Technologies (CSNT), 2011,Page(s):655 - 659

[10] A. Barth,C. Jackson, and J. C. Mitchell. Robust defenses for cross - site request forgery. [C]. In proceedings of the 15th ACM Conference on Computer and Communications Security. 2008. CCS'08 Pages(s):75 - 88

[11] Hwanjin Lee,Inkyung Jeun,Kilsoo Chun,et al. A New Anti - Phishing Method in OpenID. [C]. Second International Conference on Emerging Security Information,Systems and Technologies,2008. SECURWARE'08 Page(s):243 - 247

[12] Bansal,C. Bhargavan,K. Maffeis,S. Disvovering Concret Attacks on Website Authorization by Formal Analysis. [C],IEEE 25th Conference on Computer Security Foundations Symposium. 2012. 10. 1109/CSF. 2012. 27. Page(s):247 - 262

作者简介

张宇,(1971 -),男,博士,副研究员。主要研究方向为计算机网络、传感器网络。

胡健,(1984 -),男,硕士,主要研究方向为传感器网络。