文章编号:1671-4229(2015)03-0059-06

OAuth 授权流程的安全建模研究

林满佳, 唐　屹*
(广州大学 数学与信息科学学院, 广东 广州　510006)

摘　要: 文章实例分析基于国内开放平台的 OAuth 授权流程. 结合协议标准与网络踪迹,使用 Alloy 语言对授权流程建模,分析其中的安全问题,利用 Alloy 分析器找到了可能导致中间人攻击的漏洞,并实际验证了这个漏洞. 在此基础上,比较分析了国内其他一些开放平台的类似问题,提出了解决问题的思路.

关键词: OAuth 协议; 开放平台; Alloy 语言; 中间人攻击
中图分类号: TP 311　　**文献标志码:** A

OAuth 协议是一类授权协议,允许用户利用其在第三方站点(IDP)的帐号和口令,访问某个站点(RP). 这个协议常被用来构造开放平台,IDP 扮演着用户认证服务器的角色,RP 可以依据 IDP 的认证信息而非用户在 IDP 的帐号和口令,授权用户访问并定制访问内容,实现单点登录. 现有的 OAuth 版本为 2.0,本文所称的 OAuth 即为这个版本.

OAuth 由于使用第三方帐号登录,其安全问题一直为人们所关注. OAuth 威胁模型定义了 OAuth 2.0 安全指南[1],提供开发者可以遵循的涉及协议本身的威胁综合模型及对策. 一些形式化方法被用来确认文献[1]中涉及的安全威胁,例如,PAI 等使用 Alloy 建模语言[2],SLACK 等利用 Murphi 验证了 OAuth2.0 客户端流[3];CHARI 等利用通用可组合安全框架,分析了 OAuth2.0 的服务器流[4],但这些研究,缺乏对实现细节及应用环境的综合考虑. SUN 等对现有的 OAuth 单点登录实现进行了一些实证分析[5],但这些分析中所涉及的 IDP 不是国内流行的 IDP,而且也没有提出具体的安全隐患解决方案.

本文以国内的开放平台为基础,分析 OAuth 授权流程的安全性,笔者实证分析了腾讯 QQ 开放平台的 OAuth 授权流程,采用 Alloy 语言进行建模分析,对可能存在的安全脆弱性进行了分析与验证. 在此基础上,比较分析了国内其他一些开放平台的相关问题,提出了解决问题的一些思路.

1　OAuth 授权流程及应用实例

1.1　授权流程

OAuth 授权过程包含 4 个角色:用户 U、浏览器 B、站点 RP 以及第三方站点 IDP,其授权流程可以分为 2 类:服务器端流程(图 1)和客户端流程(图 2).

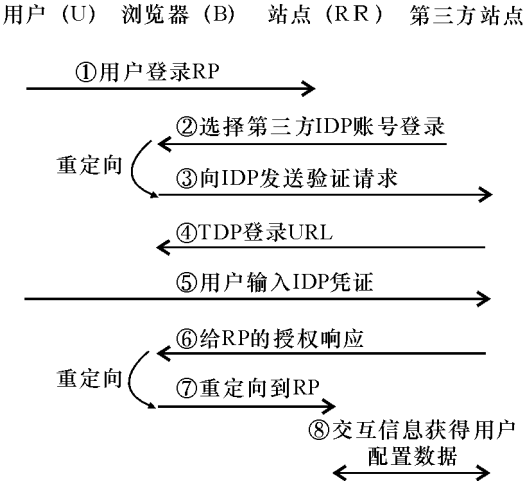

图 1　服务器端
Fig. 1　Server-side

服务器流程需要 RP 服务器端的配合. 用户向 RP 发出 IDP 帐号登录请求,RP 在收到请求后做出响应,将浏览器重定向到 IDP 进行身份验证. 在 IDP 对用户身份验证成功后,会把一个包含有表示

收稿日期: 2015 - 03 - 20;　**修回日期:** 2015 - 04 - 15
作者简介: 林满佳(1990 -),男,硕士研究生. E-mail:747374803@ qq. com
* 通信作者. E-mail:ytang@ gzhu. edu. cn

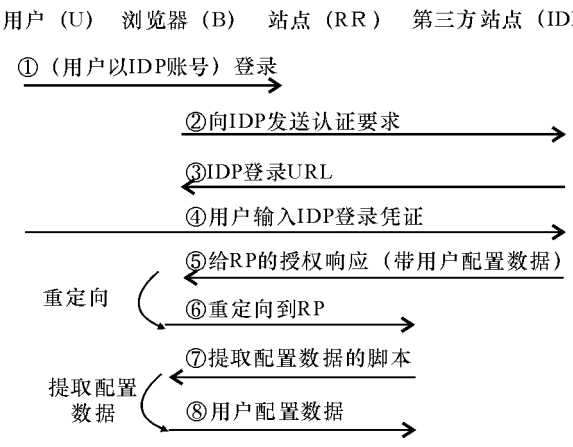

图2 客户端

Fig. 2 Client-side

对RP授权的授权码响应发回给浏览器,这时,浏览器重定向到RP,RP使用授权码与IDP进行交互以获取访问令牌,并进而访问用户的配置数据.

客户端流程无需RP服务器端的参与,但需要客户端脚本的支持. 流程开始时,用户选择用IDP账号登录,并通过浏览器向IDP发出身份验证请求. 当IDP对用户身份验证成功后,会发出一个带有用户配置数据的给RP授权的重定向响应,但用户配置数据并不直接转到RP,需要浏览器从RP下载并运行脚本,提取用户配置信息并提交给RP.

客户端流程比服务器流程更加简便,因为在IDP对用户的身份验证成功后,客户端流程的RP获得的是带有用户配置数据的响应,而服务器流程的RP在收到授权响应后还要进一步与IDP进行交互才能获得用户的配置数据. 但服务器流程相对安全,因为客户端流程直接获得的用户配置信息会暴露在浏览器上并导致泄露.

1.2 腾讯OAuth授权流程

以用户利用其QQ帐号登录酷6网站来分析腾讯OAuth授权流程.

1.2.1 浏览器从酷6重定向到腾讯

当用户选择利用腾讯QQ帐号登录酷6站点后,便开始了腾讯OAuth授权流程,首先,浏览器响应酷6的第三方登录请求,把连接重定向到腾讯的页面,其重定向的URL如下:

https://graph. qq. com/oauth2. 0/authorize? response_type = code&scope = get_user_info&client_id = 100291240&redirect _ uri = http% 3A% 2F% 2Fpasspot. ku6. com% 2Fqzone-loginCallback. htm% 3Ffrom% 3DQZONE

注意到重定向的URL包含一系列的参数:如酷6站点的ID(client_id),授权成功后的回调地址(redirect_uri)以及用户请求访问范围(scope)等.

1.2.2 腾讯验证用户的身份

腾讯收到重定向过来的信息,首先会检测相关的站点是否合法,然后展开对用户身份进行验证. 依据用户是否已处于登录状态,弹出确认页或登录页.

1.2.3 酷6获取授权码

尽管获取腾讯访问令牌的方式有2种,但在笔者的实验中仅出现服务器端的方式. 腾讯的响应将引导浏览器重定向到URL:

http://passort. ku6. com/qzone-loginCallback. htm? from = QANE&code = 0B3552DA5882A87DE06247A2337456B6

并附上授权码code. 之后酷6再使用授权码向腾讯请求访问令牌以获取用户的配置数据.

2 基于Alloy的建模分析

Alloy是一种用于描述协议或软件系统的属性和行为的声明性语言规范[6]. 利用Alloy对OAuth协议进行建模时,需要对授权过程中的每个实体建立一个签名,对有限制条件的实体增加约束事实. 这些实体可分为3类:①协议涉及的角色;②角色交互过程的参数;③协议进行授权交互时的相关的网络元素.

以对协议交互过程的参数签名为例. 在腾讯开放平台授权流程中,需要传递一些参数,如标识RP的client_id,重定向的地址redirect_uri,RP可访问范围scope,授权码code等[7]. 这些参数包含name属性和value属性,笔者定义1个包含名字和值属性对的签名attributeNameValuePair{name: Token, value: Token},然后通过这个签名派生出上述各参数.

为描述授权过程,定义以下的主要谓词.

(1) ClientRedirectsToTencent[ ]:描述浏览器由酷6重定向到腾讯的过程;

(2) UserLogin[ ]:描述用户登录腾讯站点获得授权的过程,实际实现中,由2个二选一的谓词TencentPromptsAuthorization和TencentPromptsAu-

thorizationAfterLogin 组成,分别表示未登录与已登录 QQ 的情形;

(3)ClientHasAccessToken[ ]:描述酷 6 站点获得授权码以及用户配置数据的方式,即腾讯开放平台所支持的两种授权过程,由 2 个二选一的谓词 ClientGetsServerSideAccessToken 和 TencentSendsClientSideCode 组合而成,分别表示服务器端模式和客户端模式.

对于上述的每个谓词,可以通过 run 命令检测其是否存在对应的实例. Alloy 分析器是在有限范围内搜索满足限制条件的实例,因此,在运行 run 命令的时候要指定签名的个数. 例如,运行命令 run ClientGetsServerSideAccessToken for 6 but 18 Token, 11 Time, 10 Event,表示在签名 Token 的个数≤18,Time 个数≤11,Event 个数≤10,其它签名个数≤6 的范围内搜索满足谓词 ClientGetsServerSideAccessToken 的实例,其中 Token 表示授权交互过程中所需传递参数的名字以及其对应的值,Event 表示 HTTP 请求/响应,Time 表示 HTTP 请求/响应开始和结束的时间点,可以保证 HTTP 请求/响应是顺序进行的[8].

通过 Alloy 分析器搜索,可以找到满足上述谓词的实例,即能找到服务器端流程的实例,可以直观地看出酷 6 站点获取访问令牌的过程.

3　腾讯 OAuth 授权流程存在的安全威胁

注意到在授权流程开始时,酷 6 返回给腾讯的响应信息包括:client_id、redirect_uri、scope. 这些由 RP 至浏览器的信息是通过 HTTP 传输而来并重定向,这使得攻击者可以通过中间人攻击,篡改所传输的信息. 并不是所有参数的篡改都起作用. 修改 client_id 和 redirect_uri 会导致腾讯返回错误的信息,因为 client_id 已经是在腾讯注册过了,并且 redirect_uri 是 client_id 对应主域名下的地址,所以,可以修改的是缺乏完整性保护的 scope[9].

3.1　Alloy 描述攻击行为

为了能够描述上述中间人攻击,定义签名 ProxiedHTTPTransaction,它继承于签名 HTTPTransaction. ProxiedHTTPTransaction 的主要行为就是截获客户端发给用户的响应,并对响应进行修改后发给用户.

为了证明 OAuth 存在中间人攻击,可以定义一个断言(assert),代码截图见图 3.

```
//这个断言是不成立的，因为在协议的第一阶段的确存在中间人攻击
assert NoMitmNetworkAttackPossible {
  no ptrans:ProxiedHTTPTransaction | {
    some client:Client, scope:ScopeQueryPair, granttype:GrantTypeQueryPair,
         clientid:ClientIdQueryPair, redirecturi:RedirectUriQueryPair | {
      // 中间人攻击不影响整个授权流程的进行
      ClientRedirectsToTengXun[client, scope, granttype, clientid, redirecturi, ptrans]
      // 经过中间人攻击后，重定向的Location头的中的大多数参数是不变得
      some alteredheader:(ptrans.resp.headers & LocationHeader),
           origheader:(ptrans.orig_resp.headers & LocationHeader) | {
           granttype in alteredheader.params and granttype in origheader.params
           clientid in alteredheader.params and clientid in origheader.params
           redirecturi in alteredheader.params and redirecturi in origheader.params
        // 只有客户端请求访问的范围scope发生了变化
        scope in alteredheader.params
        some orig_scope:(origheader.params & ScopeQueryPair) | {
          some ((scope.value.scopeset - orig_scope.value.scopeset) +
               (orig_scope.value.scopeset - scope.value.scopeset))
        }
      }
    }
  }
}
```

图 3　断言代码

Fig. 3　Code of assert

其中,签名 ProxiedHTTPTransaction 描述了中间人攻击的行为,即攻击者在不影响整个授权流程的情况下,修改重定向 Location 头中的 scope 参数的值,其它参数的值保持不变,结果是客户端的请求访问范围 scope 发生了变化. 在该签名前面加上关键词 no,表示该断言基于腾讯 OAuth 授权建立的模型不存在上述的中间人攻击.

最后,通过命令 check NoMitmNetworkAttack-Possible for 6 but 18 Token 对这个断言进行检测. Alloy 分析器找到一个反例,说明这个断言不成立,服务器授权流程存在中间人攻击.

3.2 攻击的验证性实验

为验证可能的攻击行为导致增加或减少客户端请求授权项. 笔者利用 webscrab 截获从酷 6 发送到浏览器的登录响应,见图 4.

图 5 利用 webscarab 修改授权信息,笔者修改响应参数里面的授权项即 scope,把它从 get_user_info 改为 all,all 表示申请腾讯 QQ 的所有权限,这就增加了授权项,修改前的授权页面见图 6,修改后的授权页面见图 7.

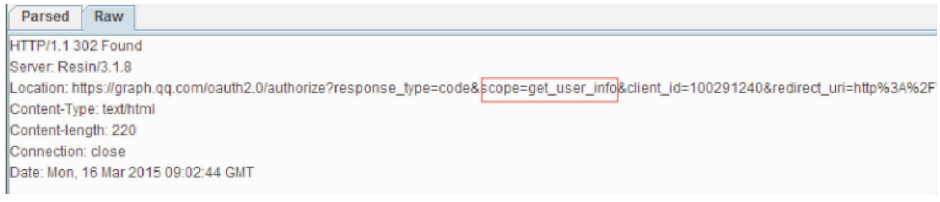

图 4 修改前的 HTTP 响应

Fig. 4 An HTTP response before modification

图 5 修改后的 HTTP 响应

Fig. 5 An HTTP response after modification

图 6 scope = get_user_info 的授权页

Fig. 6 An authorization page with scope = get_user_info

图 7　scope = all 的授权页

Fig. 7　An authorization page with scope = all

通过本实验可知,使用中间人攻击修改了授权请求中 scope 参数,使得站点向腾讯 QQ 申请的权限增加了读取、发表腾讯微博信息的权限. 用户可能会因为站点所申请的权限过大过多,而拒绝授予该站点访问自己在腾讯 QQ 中资源的权限,这就直接导致了授权的失败.

3.3　分析与讨论

社交网站由于拥有大量用户的参与,可以用作 IDP 用户认证服务器,实际上,国内的许多社交网站,都基于 OAuth 构造开放平台提供第三方的认证服务.

与腾讯 QQ 开发平台类似,新浪微博将一个最完整的授权分为 3 个步骤:登录 - 普通授权 - 高级授权. 当用户的新浪微博帐号处于登录状态时,页面会自动跳转到普通授权页,高级授权不是必须,如果开发者不申请 scope 权限,系统会自动跳过此步骤,回调应用. 由于存在高级授权页面,使得授权项的更改并不能顺利进行,因为用户可以在授权确认页中,对不想授予第三方应用的权限进行取消.

通过对开心网开放平台和人人网开放平台的测试,表明这 2 个平台并没有出现复选框要求用户进行勾选的,可以在用户不察觉的情况下修改授权项.

笔者注意到需要授权的网站 RP 通常通过 HTTP 协议向浏览器发出重定向响应的,在这响应中就包括了第三方应用所需申请得到的权限,使得攻击者可以修改 scope 参数. 解决的方案可以有①在 RP 和用户浏览器之间建立 HTTPS 连接,这就要求 RP 提供 HTTPS 服务;②在 RP 与 IDP 的通信中增加验证 scope 完整性的流程,这可以使用消息验证码来确保关键参数的完整性[10].

4　结束语

本文以通过腾讯开放平台访问酷 6 网站为例,分析 OAuth 授权流程,尤其是服务器授权流程,并在此模型的基础上进行安全性分析. 借助 Alloy 分析器,对授权流程可能存在的安全脆弱性进行分析和实证检验,提出了解决方案.

参考文献:

[1]　RFC 6819-OAuth 2.0[S]. Threat model and security considerations tools. ietf. org/html/rfc6819.

[2] PAI S, SHARMA Y, KUMAR S, et al. Formal verification of OAuth 2.0 using Alloy framework[C]//In Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT), 2011:655-659.

[3] SLACK Q, FROSTIG R. OAuth 2.0 implicit grant flow analysis using Murphi[EB/OL].[2011] http://www.stanford.edu/class/cs259/ WWW11/, 2011.

[4] CHARI S, JUTLA C, ROY A. Universally composable security analysis of OAuth v2.0[C]//Cryptology ePrint Archive, Report 2011/526, 2011.

[5] SUN S T. Konstantin Beznosov: The devil is in the (implementation) details: An empirical analysis of OAuth SSO systems [C]//ACM Conference on Computer and Communications Security, 2012: 378-390.

[6] JACKSON D. Software abstractions: Logic, language and analysis[M]. Cambridge, Massachusetts London: MIT Press, 2006.

[7] WILSON C, BOE B, SALA A, et al. User interactions in social networks and their implications[C]//Acm Eurosys, 2009.

[8] BANSAL C, BHARGAVAN K, MAFFEIS S. Discovering concrete attack on website authorization by formal analysis[C]//IEEE Comput Secur Found Sym, 2012(25): 247-262.

[9] MADEJSKI M, JOHNSON M, BELLOVIN S M. A study of privacy settings errors in an online social network[C]//IEEE Internut Confer Pervas Comput Commun Workshop, 2012(10): 340-345.

[10] HU P, YANG R, LI Y, et al. Application impersonation: problems of vauth and API design in online social network[C]//Second Edi Acm Confer Onlin Soc Network, 2014(14):271-278.

On modeling the security of oauth-based authorization

LIN Man-jia, TANG Yi

(School of Mathematics and Information Sciences, Guangzhou University, Guangzhou 510006, China)

Abstract: We model and analyze the OAuth authorization process based on an open platform instance in China. The analysis is on the combination of protocol specification and real network traces with using the Alloy language. We focus on the addressed security problems. By using the Alloy analyzer, we find a vulnerability that could be exploited to a man-in-the-middle attack. We give a proof of concept exploitation in real applications. We further discuss some other open platforms with similar experiments and propose a solution to this problem.

Key words: OAuth protocol; open platform; Alloy language; man-in-the-middle attack

【责任编辑: 陈 钢】