计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(2):212−215 [doi: 10.15888/j.cnki.csa.006199]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 CPN 的 OAuth 协议建模与分析①

张　婷[1], 张　鑫[2], 张新刚[1]

[1](南阳师范学院 计算机与信息技术学院, 南阳 473061)
[2](南阳理工学院 软件学院，南阳 473000)

摘　要: 在云计算环境下, 网络安全协议的执行环境变得更为复杂, 应用 Web 安全问题开放授权协议, 可以提高信息共享的安全性. 本文采用 CPN (Colored Petri Net) 对 OAuth 协议进行建模, 使用仿真工具 CPNTools 分析 OAuth 协议授权码模式的相关性质, 并通过仿真实验表明授权码模式可以基于令牌进行验证与授权, 防止针对授权码的 CSRF 注入攻击.

关键词: Web 安全开放授权协议; Petri 网; OAuth 协议; 协议分析

引用格式: 张婷,张鑫,张新刚.基于 CPN 的 OAuth 协议建模与分析.计算机系统应用,2018,27(2):212–215. http://www.c-s-a.org.cn/1003-3254/6199.html

Modeling and Analysis of OAuth Protocol Based on CPN

ZHANG Ting[1], ZHANG Xin[2], ZHANG Xin-Gang[1]

[1](School of Computer and Information Technology, Nanyang Normal University, Nanyang 473061, China)
[2](School of Software, Nanyang Institute of Technology, Nanyang 473000, China)

Abstract: In the cloud computing environment, the execution environment of network security protocols becomes more complex than ever before. The use of Web security issues open license agreement can improve the security of information sharing. CPN (Colored Petri Net) is employed to model OAuth protocol. The analysis of authorization code pattern in OAuth protocol adopts simulation tool named CPNTools. The experimental results show that the authorization code pattern can be verified and authorized based on token. Authorization token injection attack can be prevented in this way.

Key words: Web secure open authorization protocol; Petri network; OAuth protocol; protocol analysis

1　Web 安全开放授权协议

在云计算时代, 开放和共享数据的需求日益增加, 为了便于用户将资源授权给第三方应用, 开放授权的思想应运而生. 开放授权旨在对权限进行细粒度的控制, 并且保护用户的密码以及认证凭据. 目前主要的 Web2.0 安全开放授权机制是: OAuth 协议[1], OpenID 协议[2]和 IAM 服务[3].

OAuth 协议面向个人用户, 可对资源进行开放授权. 在线授权是其特点: OAuth 让第三方无法触及到用户的敏感信息 (如用户名与密码等), 在认证用户的资源所有者身份后, 即可以申请获得该用户资源的授权[4], 从而安全便捷地访问用户的网络资源.

OpenID 描述用户分布式方式身份认证的 URI 框架[5], 解决了传统数字身份标识管理以及认证的问题. 具有多种认证方式, 例如用户名/密码的通用认证方式, 或生物识别技术、智能卡等新型认证方式. 服务提供商不用考虑认证机制, 用户只需要注册获取 OpenID 账户, 即可在多个网站间登录, 而不需要重复注册, 便于用户统一管理身份信息[6].

IAM 服务涵盖两方面内容: 用户信息管理和用户

① 基金项目: 河南省教育厅2016年度教师教育课程改革研究项目(2016-JSJYYB-080); 河南省科技攻关项目(172102310702); 河南省教育厅科技研究重点项目 (17A520049,17A630046); 南阳师范学院校级项目 (QN2017064)
收稿时间: 2017-04-15; 修改时间: 2017-05-11; 采用时间: 2017-06-08

访问策略管理. IAM 服务采用预先授权, 用户在预先知道第三方应用所需资源请求的情况下, 授权客户端使用 REST API 方式访问资源.

2 OAuth 协议工作原理

OAuth 协议工作的基本流程[1]如图 1 所示.

(1) 用户打开客户端后, 客户端要求用户给予授权. 请求会包含以下信息: 用户的身份信息, 要访问的资源路径和操作类型等.

(2) 用户同意给予客户端授权, 并传输授权证据.

(3) 客户端向认证服务器申请访问令牌. 此时, 客户端需提供授权证据和客户端的凭证.

(4) 客户端通过认证服务器的认证后, 得到其发放的访问令牌.

(5) 客户端携带访问令牌, 向资源服务器申请获取资源. 在令牌的有效期内, 客户端可多次携带令牌访问资源.

(6) 资源服务器验证令牌的有效性后同意让客户端访问资源. 令牌的有效性包括是否过期、是否伪造、是否越权等.

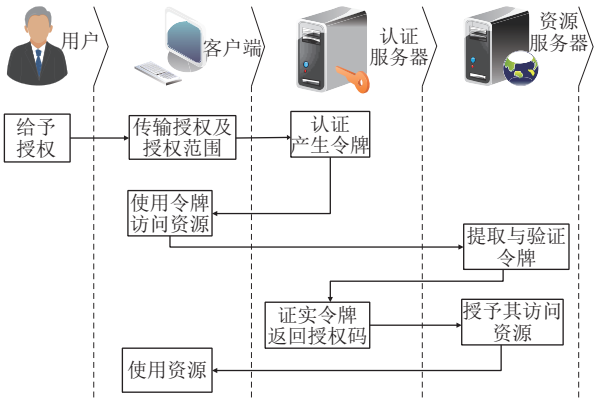

图 1 OAuth 协议工作原理

在 OAuth 2.0 中定义了四种授权方式, 如表 1 所示.

表 1 授权方式

模式名称	简介	特点
授权码模式	客户端获取授权后, 使用访问令牌与服务提供商的认证服务器进行互动.	使用最广泛、流程最严密、功能最完整的授权方式.
隐式授权模式	直接从浏览器向认证服务器申请令牌, 无需通过第三方应用程序服务器.	客户端无需认证, 可提高客户端的响应速度和效率.
客户端模式	客户端使用它的私有证书, 要求服务提供商提供服务.	不存在授权.
密码模式	客户端直接使用用户提供的用户名和密码信息, 向服务提供商索要授权.	用户对客户端高度信任.

在 OAuth 2.0 协议在使用授权码模式与认证服务器进行互动时, 使用到的各个参数如表 2 至表 6 所示.

表 2 申请认证 URI 的参数含义

参数名	含义	必选/可选
resposc_type	授权类型	必选
client_id	认证服务器分配的应用标识ID	必选
redirect_uri	用户授权操作后, 通过URI返回用户授权码	可选
scope	令牌返回时, 该参数传递申请的权限范围	可选
state	客户端当前状态, 保持请求与应答状态统一	可选

表 3 回应 URI 的参数含义

参数名	含义	必选/可选
code	授权码, 与客户端ID和重定向URI, 是一一对应关系, 只能使用一次	必选
state	与客户端的请求状态相同	可选

表 4 请求令牌的参数含义

参数名	含义	必选/可选
grant_type	授权模式	必选
code	认证服务器返回的应用授权码	必选
redirect_uri	用户授权操作后, 通过URI返回用户授权码	必选
client_id	认证服务器分配的应用标识ID	必选

表 5 返回令牌的参数含义

参数名	含义	必选/可选
access_token	访问令牌	必选
token_type	令牌类型	可选
refresh_token	刷新已过期的令牌, 获得新的访问令牌	可选
expires_in	令牌过期时间	必选
scope	权限范围	可选

表 6 更新令牌的参数含义

参数名	含义	必选/可选
grant_type	授权模式	必选
refresh_token	之前收到的更新令牌	必选
scope	申请的权限范围	可选

3 CPN 简介

Petri 网是一种基于状态的建模方法, CPN (Colored Petri Net) 是在 Petri 网基础上扩展而来, 具有概念简单性以及图形化表达的特点. Kumar 和 Spafford 将 Petri 网应用于 Web 安全领域[7], 建立了基于 Petri 网的入侵检测模型, 对入侵行为进行 CPN 建模,

当相应模型匹配的事件序列被触发时, 表示入侵行为发生.

CPN 在解决协议建模问题时具有以下的优势:

(1) 层次化. 引入了层次子网的结构, 含有替代变迁和融合库所, 可利用多个彼此联系的 CPN 网子模型构建复杂系统的整体模型.

(2) 可实现推理. 具有变迁机制, 库所被触发后变迁到达新的库所, 因果关系明确.

(3) 可处理并发或顺序性问题. 具有时间因子可以处理不同行为发生的时间.

(4) 有较完善的仿真工具, 可使用 CPNTools 工具进行可视化建模和仿真分析.

4 OAuth2.0 协议建模

4.1 OAuth2.0 协议的顶层模型

基于 CPN 的 OAuth2.0 协议顶层模型如图 2 所示, 定义模型的颜色集和变量如下:

colset DATA= String;

colset NO = INT;

colset NO*DATA =Product NO*DATA;

var success: BOOL;

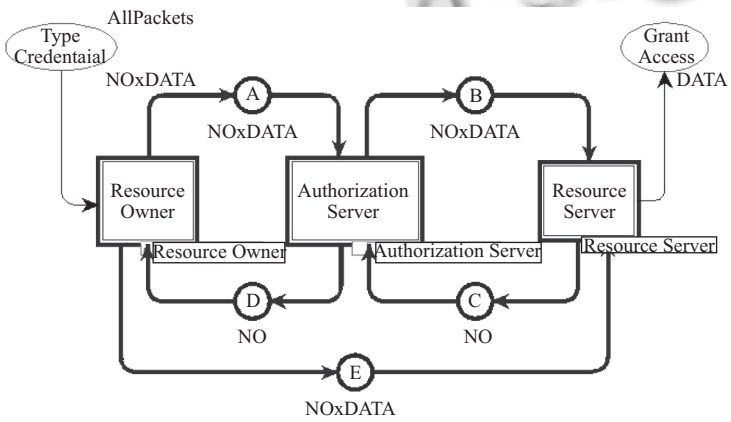

图 2 OAuth2.0 协议的顶层模型

库所 A 表示申请认证 URI, 库所 B 表示请求令牌, 库所 C 表示返回令牌, 库所 D 表示回应 URI, 库所 E 表示更新令牌. 库所 Type credential 表示授权证书, 库所 Grant Access 表示授权访问.

申请认证 URI 的参数和请求令牌的参数 (client_id, redirect_uri) 用数据类型 NO×DATA 表示, 回应 URI 的参数 (code) 用数据类型 NO 表示, 返回令牌的参数 (expires_in) 用数据类型 NO 表示, 更新令牌的参数 (refresh_token, scope) 用数据类型 NO×DATA 表示.

4.2 Resource Owner 模型

Resource Owner 的执行过程如图 3 所示. 用户访问客户端, 给客户端授权后, 认证服务器将用户导向重定向 URI, 并附授权码.

变迁 Resource Owner 表示客户端将用户导向认证服务器, 变迁 Receive Token 表示用户是否将授权给予客户端. 库所 NextToken 表示用户批准授权后发送的授权证据. 库所 Type credential 表示授权证书. 库所 A 表示申请认证 URI, 库所 D 表示回应 URI, 库所 E 表示更新令牌.

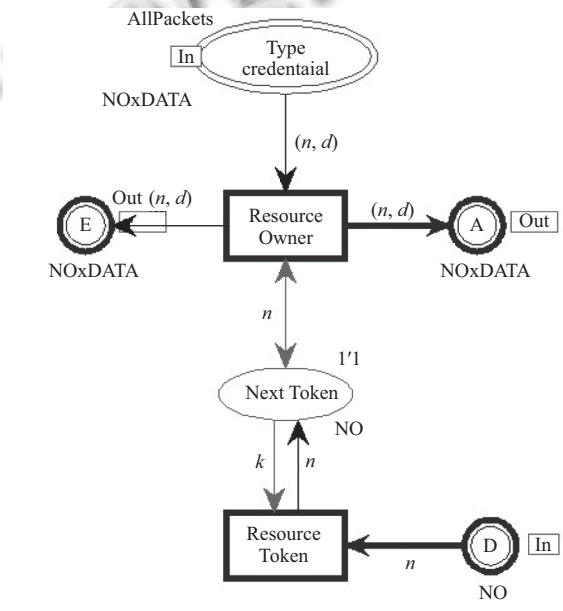

图 3 Resource Owner 模型

4.3 Authorization Server 模型

Authorization Server 的执行过程如图 4 所示. 在认证服务器确认授权码以及重定向 URI 无误后之, 将访问令牌发送给客户端.

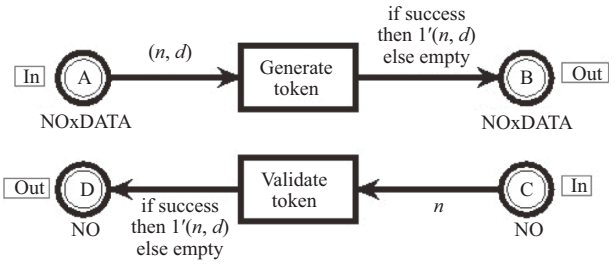

图 4 Authorization Server 模型

变迁 Generate token 表示客户端向认证服务器请求访问令牌, 变迁 Validate token 表示验证通过后, 向客户端返回访问令牌. 库所 A 表示申请认证 URI, 库所 B 表示请求令牌, 库所 C 表示返回令牌, 库所 D 表示回应 URI.

4.4 Resource Server 模型

Resource Server 的执行过程如图 5 所示. 客户端携带访问令牌访问资源服务器上的资源. 如果令牌在有效期内, 客户端可以多次访问相关资源. 资源服务器验证令牌的有效性, 通过验证后, 提供所需服务.

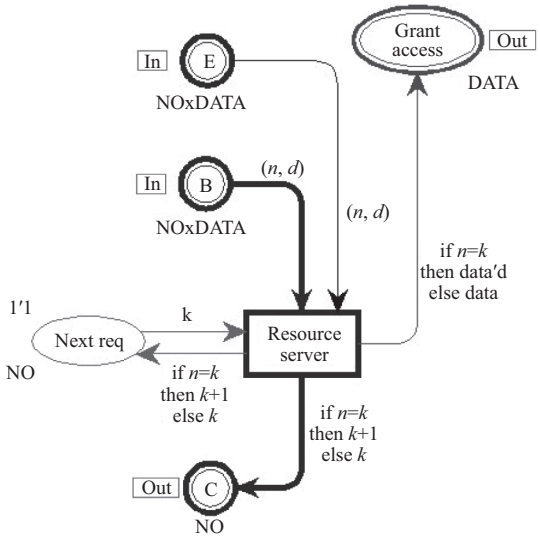

图 5 Resource Server 模型

变迁 Resource server 表示验证令牌的有效性. 库所 NextReq 表示客户端多次携带令牌访问资源. 库所 Grant access 表示授权访问相应资源. 库所 B 表示请求令牌, 库所 C 表示返回令牌, 库所 E 表示更新令牌.

5 OAuth2.0 协议分析

跨站请求伪造缩写为 CSRF, 通过在授权用户访问的页面中包含链接, CSRF 攻击可伪装用户请求, 访问受信任网站. CSRF 攻击者的目标站点常具有持久化授权 cookie 或者具有当前受信任用户的会话 cookie. 为了防范 CSRF 攻击, 需要将类似 cookie 的持久化授权方法, 转换为瞬时授权方法. 例如在 form 中包含用户授权证据作为 cookie 之外的验证.

申请认证 URI 的参数 (client_id, redirect_uri) 如果在 redirect_uri 中注入攻击者提供的 authorization_code, 模型仿真会终止在 Authorization Server 的变迁 validate token 执行过程中, 不会访问资源服务器上的资源. 这说明从浏览器安全角度考虑, OAuth 协议在 redirect_uri 中引入 state 参数可以防范 CSRF 攻击. 如果没有 state 参数, 攻击者可能导致客户端访问错误的资源.

6 小结

本文列举了主要的几种 Web 安全开放协议, 绘制了 OAuth 协议时序图, 使用 CPN 对 OAuth2.0 协议的授权码模式进行层次化建模. OAuth2.0 协议的模型包括顶层模型、Resource Owner 模型、Authorization Server 模型和 Resource Server 模型. 并使用 Petri 网仿真工具 CPNTools 对 OAuth2.0 协议进行了仿真分析, 直观地展现协议运行过程和防范 CSRF 攻击的特点.

参考文献

1 The OAuth 2.0 authorization protocol (draft-ietf-oauth-v2-16). http://tools.ietf.org/html/draft-ietf-oauth-v2-16. [2011-05-19].
2 Recordon D, Reed D. OpenID 2.0: A platform for user-centric identity management. Proceedings of the 2nd ACM Workshop on Digital Identity Management. Alexandria, VA, USA. 2006. 11–16.
3 胡刚, 郭文奇, 戚前方. IAM 安全技术在开放平台系统管理的应用. 计算机工程, 2005, 31(S1): 192–194.
4 李馥娟. 基于 OAuth 的开放授权技术及在云计算中的应用. 计算机系统应用, 2015, 24(4): 228–232.
5 夏晔, 钱松荣. OpenID 身份认证系统的认证等级模型研究. 微型电脑应用, 2011, 27(4): 7–9.
6 刘润达, 王卷乐, 杜佳. OpenID: 一种开放的数字身份标识管理及其认证框架. 计算机应用与软件, 2008, 25(12): 127–129. [doi: 10.3969/j.issn.1000-386X.2008.12.043]
7 Kumar S, Spafford E H. A software architecture to support misuse intrusion detection [Technical Report]. CSD-TR-95-009. West Lafayette, USA: Purdue University, Department of Computer Sciences, 1995.