文章编号:1000-5641(2015)S1-0240-06

高校信息化环境下 OAuth 授权体系的研究与实践

白雪松, 杜晋博, 王 罡
(上海交通大学 网络信息中心, 上海 200240)

摘要: 随着互联网技术的快速发展,高校信息化环境下建立的传统授权体系遇到了很多挑战. 本文以上海交通大学 OAuth 授权体系的实践为基础,研究 OAuth 授权模型,并对高校信息化环境下 OAuth 授权体系实践中遇到的问题进行了探讨.

关键词: OAuth; 授权体系; 权限控制
中图分类号: TP393.08 **文献标识码**: A **DOI**:10.3969/j.issn.1000-5641.2015.z1.038

Research and practice on the OAuth authorization system under university information environment

BAI Xue-song, DU Jin-bo, WANG Gang
(*Network & Information Center, Shanghai Jiao Tong University, Shanghai* 200240, *China*)

Abstract: With the rapid development of the Internet technology, the traditional authorization system under a university's information technology environment encountered many challenges. This paper, based on the practice of the Shanghai Jiaotong University OAuth authorization system, does research on OAuth authorization model, and discusses problems encountered in the practice of building OAuth authorization system under the university's information technology environment.

Key words: OAuth; authorization system; access control

1 高校信息化进程中的传统授权体系

随着高校信息化进程的不断推进,各高校普遍建立了比较完整的认证和权限控制模型,很多高校也根据自身特点建立了授权体系,实现了集中授权和分级授权相结合的授权机制. 传统的权限控制模型一般遵循目前权限系统中通用的 RBAC 规范,上海交通大学结合高校信息化建设的需要,在 RBAC 规范的基础上,扩展了 RBAC 规范,既确保了通用性,又保证了能更好地符合高校信息化建设的实际[1].

RBAC 模型作为目前最为广泛接受的权限模型,是由 NIST (The National Institute of

收稿日期:2014-10
第一作者:白雪松,工程师,研究方向为认证授权. E-mail:dinosissi@sjtu.edu.cn.

Standards and Technology，美国国家标准与技术研究院）提出的[2]. 它由 4 个部件模型组成：基本模型 RBAC0(Core RBAC)、角色分级模型 RBAC1(Hierarchal RBAC)、角色限制模型 RBAC2(Constraint RBAC)和统一模型 RBAC3(Combines RBAC).

在 RBAC 之中，包含用户 users(USERS)、角色 roles(ROLES)、目标 objects(OBS)、操作 operations(OPS)、许可权 permissions(PRMS)五个基本数据元素，权限被赋予角色，而不是直接被赋予用户. 当一个角色被指定给一个用户时，此用户就拥有了该角色所包含的权限. 会话 sessions 是用户与激活的角色集合之间的映射. RBAC0 与传统访问控制的差别在于增加一层间接性带来了灵活性，RBAC1、RBAC2、RBAC3 则是先后在 RBAC0 上的扩展.

RBAC0 模型如图 1 所示，其中定义了能构成一个 RBAC 控制系统的最小的元素集合.

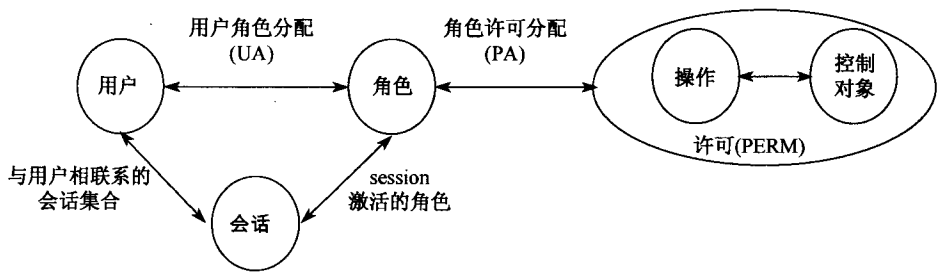

图 1　RBAC 0 模型

但是，RBAC 模型通常关注的是单个系统的权限体系，在高校的信息化实践中，普遍存在跨应用的授权需求. 我们认为，统一授权模型不应该仅限于考虑将原本在各个业务系统的授权简单集成在统一授权系统中，而应该考虑将统一授权系统作为一个各业务系统的角色、权限的集合，设计出一套高于各业务系统的统一的角色和授权体系，使得各业务系统能够共享这些角色. 在此理念下，我们在授权体系中引入了全局角色的概念[3].

2　传统授权体系面临的问题

随着各高校信息化的快速发展，高校中的应用已经发生了很大的变化，特别是移动应用的爆发式发展，使得传统的认证和授权模型已经越来越难以满足应用发展的需求. 我们所面临的主要有以下几个方面的问题：

(1) 原来大多数的应用都是各高校自主开发或引进的和教学、科研、行政等有关的核心业务系统，随着高校信息化和互联网应用的快速发展，接入的应用大大增加，开发者从以前的核心业务部门、少数软件供应商，扩大为广大学生开发者、互联网服务提供商、独立开发者等，这些开发者也需要申请使用资源，单纯的统一身份认证和基于 RBAC 的授权体系已经难以满足当前的高校软件生态环境.

(2) 传统的授权体系基本都是系统级的授权，即直接对应用进行授权. 以学生的选课信息为例，在传统的模式中，我们会授权某个应用可以使用所有学生的选课信息，这个应用通常是由高校自主开发或者引进的可以被系统级授信的系统，但在现有的模式中，存在大量无法被系统级授信的应用，比如某学生开发的移动 APP，如果仍然使用传统的资源访问控制体系显然是不合适的，更合适的做法是给使用这个 APP 的用户提供足够的信息，让用户自主决定是否信任这个应用，是否允许这个应用获取他的选课信息.

(3) 移动应用已经成为一个不可逆转的趋势,移动应用和一般的 Web 应用不同,通常有一个比 Web 更强大的客户端,高校原有的统一身份认证体系多是基于 Web 的特性设计的,和移动应用的整合过程中也遇到了很多实际的困难.

(4) 互联网上已经有大量的应用实现了和 OAuth 协议的整合,要引入这些应用时,由于高校中传统的资源控制方案都不是以通用协议的方式来设计的,所以需要做很多额外的定制化工作.

3 OAuth 授权模型

正是基于以上的原因,上海交通大学引入了标准的 OAuth 协议,支持 OAuth 1.0a 协议的服务目前已经正式上线运行 3 年左右,支持 OAuth 2.0 协议的服务也已经推出了一段时间.从上海交通大学 OAuth 1.0a 运行的情况来看,OAuth 已经从开始时对统一身份认证体系的补充,逐渐发展为资源访问控制的核心解决方案.

3.1 OAuth 授权的基本思路

OAuth 是一个开放的授权协议,允许第三方应用在没有资源所有者密码的情况下,通过服务提供方颁发的有时效性的令牌(Access Token)访问服务提供方中的某些用户资源.OAuth 授权的基本思路如下(参见图 2).

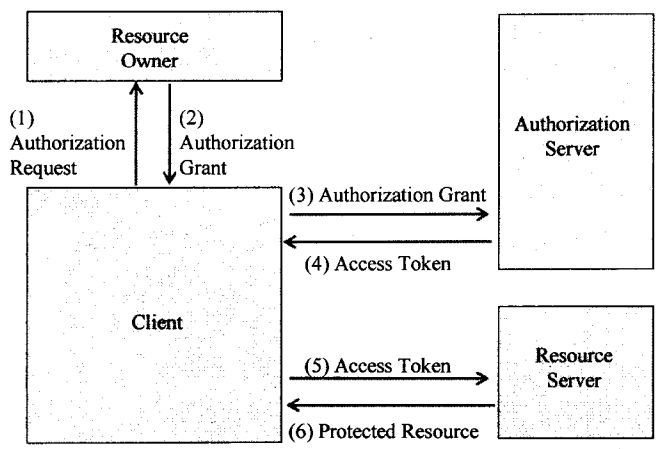

图 2 OAuth 授权的基本思路[4]

(1) 第三方应用请求资源所有者的授权,请求中一般包含:要访问的资源路径,操作类型,第三方应用的身份等信息.

(2) 资源所有者批准授权,并将"授权证据"发送给第三方应用.典型的做法是,授权服务器提供授权界面,让资源所有者显式授权.

(3) 第三方应用向授权服务器请求 Access Token.此时,第三方应用需向授权服务器提供资源所有者的"授权证据",以及第三方应用自己身份的凭证.

(4) 授权服务器验证通过后,向第三方应用返回 Access Token.

(5) 第三方应用携带 Access Token 访问资源服务器上的资源.在令牌的有效期内,第三方应用可以多次携带令牌去访问资源.

(6) 资源服务器验证令牌的有效性,比如是否伪造、是否越权、是否过期,验证通过后,

才能提供服务.

3.2　OAuth 协议简介

目前有两个不兼容的协议版本：OAuth 1.0a 和 OAuth 2.0. 一个典型的 OAuth 1.0 认证授权过程通常包括三种角色，分别是：

(1) Consumer：消费方，可以理解为需要使用用户资源的第三方应用.

(2) Service Provider：服务提供者，即 OAuth 服务提供方.

(3) User：用户，即用户资源的所有者.

OAuth 1.0 认证授权的主要三个步骤是获取未获用户授权的 Request Token，获取用户授权的 Request Token，用授权的 Request Token 换取 Access Token. 当应用拿到 Access Token 后，就有权访问用户授权的资源了. 具体的授权过程参见 RFC5849[5].

OAuth 1.0 协议在实际应用中遇到了一些问题，主要是以下两点：其一，签名逻辑过于复杂，对开发者不够友好；其二，授权流程太过单一，除了 Web 应用以外，对桌面、移动应用来说不够友好. 为解决这些问题，OAuth 2.0 做了以下改变：

(1) 去掉签名，改用 SSL(HTTPS)确保安全性，所有的 token 不再有对应的 secret 存在，这也直接导致 OAuth 2.0 不向前兼容 OAuth 1.0.

(2) 针对不同的情况使用不同的授权流程，和 OAuth 1.0 只有一种授权流程相比，OAuth 2.0 提供了多种授权流程，可依据实际情况选择.

OAuth 2.0 的参与实体通常包括以下四种.

(1) RO (resource owner)：资源所有者，对资源具有授权能力的人，相当于 OAuth 1.0 中定义的 User.

(2) RS (resource server)：资源服务器，存储资源，并处理对资源的访问请求.

(3) Client：第三方应用，它获得 RO 的授权后便可以去访问 RO 的资源，相当于 OAuth 1.0 中定义的 Consumer.

(4) AS (authorization server)：授权服务器，它认证 RO 的身份，为 RO 提供授权审批流程，并最终颁发 Access Token. 为了便于协议的描述，逻辑上把 AS 与 RS 区分开来，物理上 AS 和 RS 可以由同一服务器来提供服务，也可以由不同的服务器来提供服务.

OAuth 2.0 为了支持不同类型的第三方应用，提出了多种授权类型，如授权码 (Authorization Code Grant)、隐式授权 (Implicit Grant)、RO 凭证授权 (Resource Owner Password Credentials Grant)、Client 凭证授权 (Client Credentials Grant)等[6].

4　上海交通大学的 OAuth 实践

OAuth 是开放协议，业内已有很多成熟的系统实现可供借鉴. 但建设一套以 OAuth 为核心的授权体系，远非实现一个符合 OAuth 协议的服务端这么简单，还需要有很多与之配套的建设内容. 本文结合上海交通大学近年来的实践，简要介绍下 OAuth 授权体系建立中的几个重要问题，以及我们对这些问题的思考.

4.1　与统一身份认证系统的整合

理论上讲，认证(Authentication)和授权(Authorization)有着严格区别，在上海交通大学的实践中，负责认证的统一身份认证体系(jAccount)和负责授权的 OAuth 权限控制体系也被设计为两个独立的体系. 但由于历史原因、用户使用习惯、用户教育等因素，在我们的实

践中,OAuth 协议中对用户进行认证的部分仍然使用原有的统一身份认证体系,即 jAccount 只负责认证、OAuth 只负责授权. 在上海交通大学整体的认证授权模型中,OAuth 被当成是一个使用 jAccount 认证的第三方应用,如果用户在会话期内登录过使用 jAccount 认证保护的系统,用户将漫游到 OAuth 的授权界面;如果用户在会话期内没有访问过 jAccount,会首先引导用户 jAccount 登录,再进入授权界面. 这样的方式即简化了 OAuth 权限控制模型的实现,也符合传统的用户使用习惯.

4.2 API 建设

OAuth 权限控制模型的最根本出发点是对用户资源的保护,用户资源在整个 OAuth 权限控制体系中对应的就是大量的 API,如果没有强有力的 API 建设,可以被 OAuth 保护的用户资源太少,就会极大的影响 OAuth 的推广. 目前我们已经建立了约 40 个 scope 的 RESTful 风格 API,范围覆盖高校信息化中常见的多个领域.

与此同时,我们对重要业务系统的建设和升级也提出了 API 建设要求,在我们重要的业务系统建设规划中,除了业务系统本身要实现的业务需求以外,会增加建设符合上海交通大学建设规范 API 的要求. 随着 API 建设的推进,在 OAuth 权限控制模型下可保护的用户资源也会越来越丰富,这对于整个高校的软件生态也会带来积极的影响.

4.3 scope 管理

OAuth 1.0a 协议中并没有引入 scope,但是在实践中,我们和其他主流的 OAuth 服务提供商一样,引入了 scope 的概念——scope 就是第三方应用拿到的 AccessToken 可以访问的资源范围. 第三方应用在提交应用申请时,需要提交可能访问的最大 scope 范围,虽然 OAuth 权限控制模型中,用户会对自己的资源访问许可负责,但我们认为在高校的信息化建设实践中,如果第三方应用申请的 scope 包含用户的敏感资源,还是需要管理员的审核才可以通过申请,注册完成后第三方应用申请用户资源时还需再次由用户进行授权. 第三方应用在提交 scope 申请时,还需要指明必需的 scope,即用户若想访问该应用必须授权的 scope,如果用户未颁发给第三方应用这些 scope,将无法正常访问第三方应用,另外的 scope 将作为可选 scope,由用户根据自身需要选择性颁发资源访问许可.

Scope 列表是由我们可以提供的 API 范围决定的. 在目前上海交通大学的 API 体系中,scope 主要包括以下几类:

(1) 用户信息(基本信息、身份信息、联系信息等);

(2) 消息与任务推送(channel 包括 Email, SMS, Web 等);

(3) 非结构化存储;

(4) 教学(课程、考试、成绩等);

(5) 社交(群组、关注等);

(6) 表单工作流.

4.4 应用管理

引入 OAuth 权限控制体系,对高校信息化的软件生态产生了重大影响,原有的应用管理模式也需要随之改进. 引入 OAuth 后,我们从原来只需要管理少量教务、科研等主流核心业务系统应用级别的权限,扩展为管理大量互联网应用和独立应用的用户资源访问控制权限. 在这样的背景下,如果仍然以原有的方式管理应用,权限审核的难度将大幅增加,这也不符合高校信息化和互联网发展的潮流. 同时,由于开发者的不可控,从应用级别管理授权的

模式已经走不通了，必须与 OAuth 权限控制体系相结合，建设新的应用管理模式.

和主流互联网服务提供商（如新浪、腾讯、百度等）一样，我们也对申请接入的应用做了分类，如果只需要简单资源，比如用户基本信息等资源的应用，可以由开发者全程自助完成应用申请，管理员事后审核，增加了应用接入的灵活性. 如果申请的资源包含敏感资源，开发者需要提交应用的主要功能和需要这些用户资源的场景，由管理员按实际情况允许或拒绝应用接入.

[参　考　文　献]

[1] 白雪松，茅维华，身份与权限体系关键技术的总体设计与实践[J]. 中山大学学报，2009(S1)：260-263.

[2] SANDHU R, FERRAIOLO D, KUHN R. The NIST Model for Role-Based Access Control: Towards A Unified Standard[EB/OL]. [2014-10-31]. http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf

[3] 白雪松，蒋磊宏，茅维华，全局角色在统一授权体系中的应用[J]. 实验技术与管理，2011(6)：116-118.

[4] OAuth core Workgroup. OAuth Core 1.0[EB/OL]. 2007[2014-11-01]. http://oauth.net/core/1.0.

[5] IETF. The OAuth 1.0 Protocal[EB/OL]. 2010[2014-11-01]. http://tools.ietf.org/html/rfc5849.

[6] IETF. The OAuth 2.0 Authorization Framework[EB/OL]. 2012[2014-11-01]. http://tools.ietf.org/html/rfc6749.

（责任编辑　王善平）