基于 OAuth 的开放授权技术及在云计算中的应用①

李馥娟

(江苏警官学院 计算机信息与网络安全系, 南京 210031)
(江苏警官学院 网络管理中心, 南京 210031)

摘 要: 在云计算中, 传统应用系统中使用的基于单一安全域的身份认证和资源授权模式已无法适应复杂环境中的管理要求, 需要制定跨域访问的安全控制策略. 在重点分析了云计算中数据安全和隐私保护所遇到的挑战的基础上, 有针对性地介绍了OAuth2.0协议的原理和功能特点, 提出了开放授权技术在云计算中的应用优势, 并通过一个工程应用实例讨论了具体的实现方法和思路.

关键词: OAuth2.0; 云计算; 授权; 开放标准

OAuth Technology and its Application in the Cloud Computing

LI Fu-Juan

(Department of Computer Information and Network Security, Jiangsu Police Institute, Nanjing 210031, China)
(Center of Network Management, Jiangsu Police Institute, Nanjing 210031, China)

Abstract: Cloud computing is a complex network environment, and traditional applications use authorization and authentication based on a single security domain mode, it does not meet the requirements of cloud computing, cloud computing needs to establish cross-domain security access control policy. Based on the analysis of the challenges of data security and privacy protection in the cloud computing, this paper introduces the principle and function of the OAuth2.0 protocol, and points out the OAuth2.0 advantage of open license technology and its application in the cloud computing. Finally, through a cloud computing example, the implementation methods and development ideas had been discussed.

Key words: OAuth2.0; cloud computing; authorization; open standards

云计算是一种计算和服务模式, 它以互联网和数据中心为基础, 利用虚拟化技术构建由计算资源、存储空间、应用程序等组成的可共享资源池, 为用户提供按需、便捷、可扩展的服务, 而不用关心数据中心管理、数据处理、应用程序部署等技术细节[1-2]. 近年来, 随着YouTube、Facebook、Twitter、腾讯QQ空间、人人网、新浪微博等国内外社交网络(Social Networking Services, SNS)的飞速发展, 更从应用层面加速了云计算的实践探索与创新. 由于云计算具有的开放标准、分布式部署、按需分配资源、泛在接入等特点, 以身份认证和资源授权管理为代表的大规模跨域管理便成为安全研究的重点.

与此同时, 在信息化的推动下, 许多高校、政府部门、科研机构、企业根据各自的工作需要分别建立了自己的应用系统, 并积累了大量宝贵的数据资源. 随着网络应用的不断开放, 原来的相对封闭的系统面临着相互间以及与 Internet 上 SNS 间的对接, 进一步整合和优化资源, 实现应用价值和效率的最大化. 然而, 资源建设者、使用者和技术开发人员, 都不想轻易摈弃原有的身份认证和资源授权模式, 希望在开放授权与系统改造升级两者之间求得暂时的平衡, 渐进式地改变用户已形成的信息化应用习惯和体验. OAuth2.0 协议正是在这一背景下应运而生, 并很快引起了云计算开放授权领域的关注.

本文在简要分析当前云计算尤其是企业私有云和混合云平台建设基本需求和特点的基础上, 结合 OAuth2.0

① 基金项目:江苏省高等学校重点学科建设专项;2013 年江苏省高等教育教改研究立项课题(2013JSJG150)
收稿时间:2014-08-04;收到修改稿时间:2014-10-16

协议的功能和应用优势，以江苏警官学院在研的“基于云计算的战、学、研信息资源共享平台建设与应用”项目的具体实践为例，提出了一个基于 OAuth2.0 的云计算开放授权管理模型，不但解决了本单位内部网络资源系统(主要有教务管理系统、网络教学平台、科研管理系统等)的整合问题，而且实现了与部分兄弟院校系统之间的对接，并为与全省数字图书馆系统以及基于 Internet 的 SNS 实现开放身份认证提供了相应的安全接口.

1 云计算资源授权遇到的挑战

云计算是一个由多个单一安全域通过轻耦合方式联合而成的逻辑安全域，云计算所具有的可扩展性、开放性和管理的复杂性，使访问控制变得非常繁杂，传统单一安全域中的访问控制模型和机制无法解决多域环境中可能出现的安全威胁及管理复杂化. 在云安全联盟(cloud security alliance, CSA)确定的 15 个云计算重点技术中，认证和访问管理位列其中[3].

1.1 挑战 1: 域间授权互操作机制的建立，既要兼顾单一域下的资源访问模式，又要体现云平台的统一认证功能

任何一个多用户系统都涉及到身份认证和资源授权问题[4]. 在传统的单一安全域中，一般都存在技术上成熟、运行稳定的用户和资源管理模式来负责协调管理本域中的不同应用系统，如基于单点登录(Single Sign On, SSO)的统一身份认证系统实现了用户在单一安全域内的一次登录多次访问能力. 在云计算环境中，应用系统多属于不同的安全域，多数访问需要跨域进行，因而需要一个云计算统一身份认证(也称为“联邦身份认证”)中心负责对逻辑安全域中的用户身份和资源授权进行统一管理. 云计算统一身份认证需要建立基于逻辑安全域的认证授权策略，在进行资源访问时，各安全域保持原有的访问控制机制，跨域访问则由云计算统一身份认证中心进行集中管理. 这一模式符合当前云计算的建设和应用实际，否则如果一味地追求基于整个逻辑安全域的高度集中的控制而轻意放弃各安全域中已使用的策略，无论是用户习惯、管理方式，还是技术实现都不现实，需要一个渐进式的调整与融合过程. 然而，在过渡期间，在坚持域内自治、域间协作的前提下，如何针对相对分散的共享资源建立一个安全可靠、彼此互信、相互认可的访问控制策略，需要在继承单一安全域已有技术的同时，针对云计算环境的域间授权互操作机制进行技术上的突破和应用中的创新.

1.2 挑战 2: 云计算环境下安全边界的不清大大增加了对数据安全和隐私保护的难度

任何安全技术的应用和安全产品的部署都需要针对具体的安全边界，明晰的边界是实施安全管理的前提. 虽然层次和功能清晰的云计算体系结构已见雏形，但因层间的轻耦合性而导致的安全边界的不稳定性和模糊性，大大增加了云计算中对数据安全和用户隐私保护的难度，传统单一安全域中的安全机制在其可扩展性和资源按需分配方面无法满足多域环境下的需求，并暴露出一些安全问题. 例如，IaaS层中的虚拟技术在有效隔离用户隐私方面存在安全隐患[5]，PaaS层的海量数据处理也存在对用户信息的泄露风险[6]，在SaaS层，共享服务器中存放的敏感数据在访问控制方面存在安全漏洞[7]. 类似以上问题，充分表明单一安全域中的安全控制机制已经不能适应多域环境下的管理需求. 同时，传统网络中的安全管理问题在云计算中仍然存在.

1.3 挑战 3: 域间差异性为跨域访问中的隐私保护增加了难度

隐私保护和数据安全是云计算安全领域中最为突出的两个问题[8]. 云计算跨越了多个不同的安全域，每个安全域都是一个自治系统，安全域之间存在软硬件结构的异构性、管理模式的差异性和资源的多机构共享性，不同安全域间通过细粒度控制实现对访问的约束. 然而，单一安全域中的用户身份管理技术和资源授权策略无法满足云计算中跨越不同自治域的用户信息安全管理要求，尤其在进行跨域访问时，用户身份和访问习惯等隐私很容易被记录和分析，甚至成为地下灰色产业链的信息源头. 同时，由于用户数据出现在异地空间，过程数据和不需要的数据是否被彻底删除，这些操作在本地无法得到有效的监控.

2 OAuth2.0授权管理模式

随着以 Web 应用为核心的云计算的快速发展，主要针对为用户提供开放授权管理的 OAuth(Open Authorization，开放授权)协议在自身的不断完善中引起关注. 相对于 OAuth1.0/1.0a 两个版本，OAuth2.0 在技术细节和功能定位上都进行了较大改进甚至是彻底改变，成为一个相对独立的开放授权标准. 为此，本文仅以 OAuth2.0 为基础进行介绍.

2.1 OAuth2.0 协议

OAuth2.0[9-11]定义了 4 种不同的角色: RO(resource owner, 资源拥有者)、RS(resource server, 资源服务器)、Client(客户端)和AS (authorization server, 授权服务器). 其中, RO是指能够对受保护资源进行授权的实体. 根据授权管理需要, 当以“在线授权”方式手动执行授权操作时, 该实体是指具有授权操作管理能力的管理人员, 当以“离线授权”方式由系统自动进行授权操作时, 该实体为具有授权操作管理功能的一个管理程序; RS用于存放受保护资源, 并对资源的访问请求作出应答; Client指第三方应用系统或程序, 它事先与AS之间建立信任关系, 其域内用户在得到RO的授权许可后便可以去访问RS上的资源. Client可以是一个Web站点、一段JavaScript代码或安装在本地的一个应用程序, 不同的Client类型可使用不同的授权类型进行授权, 如授权码许可(authorization code grant)授权、Client凭证许可(client credentials grant)授权等; AS用于对RO的身份进行验证和资源授权管理, 并颁发访问令牌(access token). 在具体应用中, AS和RS一般由同一个服务器来提供服务. 如图 1 所示, OAuth 2.0 协议的基本工作流程如下:

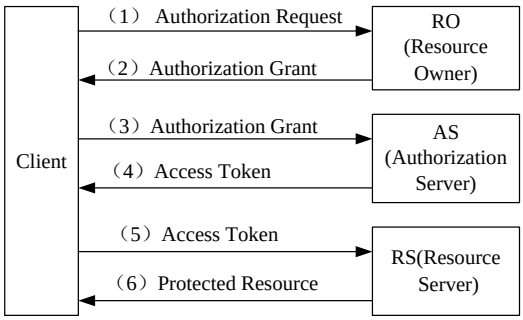

图 1　OAuth 2.0 协议基本工作流程

(1) Client 向 RO 发送“授权请求”(authorization request), 请求报文中一般包含要访问的资源路径、操作类型、Client 的身份等信息;

(2) RO 同意 Client 的授权请求, 并将“授权许可”(authorization grant)发送给 Client. 根据授权管理需要, AS 会为 RO 提供权限分配操作界面, 让 RO 进行细粒度在线授权操作, 或根据事先约定的授权管理策略, 由系统自动完成离线授权操作;

(3) Client 向 AS 请求“访问令牌”(access token). 此时, AS 需要验证 Client 提交给自己的“授权许可”, 并要求 Client 提供用于验证其身份的信息;

(4) AS 在通过对 Client 的身份验证后, 便向它返回一个“访问令牌”, 只有持有访问令牌的 Client 才能访问资源;

(5) Client 向 RS 提交“访问令牌”;

(6) RS 验证“访问令牌”的有效性, 具体由令牌的颁发机构、令牌颁发日期、时间戳等属性决定. 当验证通过后, 才允许 Client 访问受保护的资源. 其中, 在令牌的有效期内, Client 可以多次携带同一个“访问令牌”去访问受保护的资源.

2.2 OAuth2.0 开放授权模式与云计算相结合的特点

OAuth2.0 协议与云计算的有机结合具有以下几方面的优势:

(1) OAuth 授权机制为逻辑安全域中单一安全域之间的授权互操作提供了一套具体有效的方案, 符合当前云计算资源授权模式的需要, 单一安全域中已有的身份认证和授权管理方式可以继续使用, 跨域授权操作则由 Authorization Server 统一管理. 这样, 一方面解决了多系统之间的开放授权问题, 另一方面最大限度地保留了原有单一安全域中的用户体验, 在开放与继承之间取得了一个平衡;

(2) OAuth 作为一个开放授权协议, 其应用符合当前云计算中域间授权互操作的轻耦合特点, Authorization Server 的部署没有强制性, 任何资源服务提供者都可以组建自己的 Authorization Server, 并经协商为本逻辑安全域中的第三方提供授权服务. Authorization Server 的可靠性和可信性在很大程度上决定着开放授权中用户信息的安全性, 在当前大家普遍关注隐私保护的大背景下, OAuth2.0 协议所具有的松耦合特点消除了用户的安全顾虑;

(3) 按需分配资源是云计算的一大特点和应用优势, 也符合跨域操作中按用户角色分配资源的要求. OAuth 提供的基于细粒度的授权控制方式, 满足了云计算按需分配资源的管理要求;

(4) 在 OAuth 协议的整个授权过程中没有直接用到第三方(Client)及域内用户的私有信息, 而是使用“访问令牌”和数字签名方式, 提高了协议的安全性, 最大限度地实现了对用户隐私的保护. 目前, 大量的互联网协议(如 TCP、SSL 等)在工作过程中都需要交换用户信息, 这一机制存在较大的安全隐患, 而 OAuth2.0 则利用“访问令牌”解决了交互过程中的安全

问题;

(5) OAuth 通过安全的 API 为云环境中各类固定和移动终端提供泛在接入的访问授权服务, 最大限度地发挥了协议的开放性和兼容性.

作为一个开放标准的联合授权协议, OAuth2.0 协议一经推出便引起了云计算中联合授权管理的关注, 目前不仅仅开始应用于 SNS, 而且在私有云环境中正在发挥其功能优势, 并可以与 OpenID、SAML 等多种身份认证技术配合实现开放标准的基于 SSO 的授权服务.

3 基于OAuth2.0的授权应用实例

目前, OAuth 2.0 已经成为开放平台认证授权的事实上的标准. 作为一个开放性的授权管理协议, 不仅在公有云计算环境中可以直接使用 SNS 中的 OAuth 授权服务系统, 而且在私有云环境中也可以组建自己的授权服务系统, 为云计算不同单一安全域中的用户提供分布式的跨域授权服务.

3.1 跨域授权访问操作的实现方法

图 2 所示的本单位研究项目中基于 OAuth2.0 跨域授权的一个模型, 其中 abc.net 和 xyz.com 分别属于不同的安全域. 为便于表述, 其中 abc.net 代表某一兄弟高校的域名, 而 xyz.com 代表江苏警官学院的域名, 同时将 AS 服务器创建在 xyz.com 所在域名内, 由该 AS 同时向 xyz.com 和 abc.net 域内的用户提供授权服务.

现在, 作为 Client 的 abc.net 需要 xyz AS 对其用户进行授权来访问 xyz.com 上的受保护资源 xyz RS, RO 通过 Web 浏览器进行操作. 为了实现此功能, abc.net 事先在 xyz AS 上进行了注册, 获得了 Client 标识符 client_id 和共享密钥 client_secret. 整个跨域授权操作流程如下:

(1) 站点 abc.net 所在安全域中的用户通过用户代理以 www.xyz.com 链接方式(注意: 该流程在图 2 中未标出)请求访问 xyz RS 上的资源. 该请求信息被指向 RO;

(2) 通过 http 302 将 RO 用户代理重定向到 AS. 其中, abc.net 在重定向 URI(redirect_uri)中携带了用于在 xyz RS 上标识自己的 client_id 标识符(一般为一段数字代码), 以及访问类型 access_type、被访问范围 scope、审批提示 approval_prompt 等参数. 例如, 当 approval_prompt=force 时将要求对 Client 的本次访问请求进行在线授权, 当缺少该参数时将由系统进行默认的离线授权;

(3) AS 要求 RO 提供其身份验证信息, 实现对其身份合法性的验证. 同时, AS 还会向 RO 提供一个用于决定是否同意 abc.net 的本次请求的审批界面(当 approval_prompt=force 时);

(4) RO 向 AS 提交身份认证信息;

(5) 当验证 RO 身份的合法性后, AS 将向 Client 发送一个授权码 authorizaton_code, 并根据步骤(2)中提供的 redirect_uri, AS 将 RO 的身份代理重定向到 Client;

(6) Client 向 AS 提交 authorizaton_code, 请求换取 AS 的 access_token. 该请求信息中携带有用于 Client 身份信息的 client_id 以及步骤(2)中的 redirect_uri 等参数, 用于证明自己的身份;

(7) AS 在接收到 authorization_code 后, 提取其中的 client_id 和 redirect_uri, 以此对 Client 的身份进行双因子验证;

(8) 当通过身份认证后, AS 向 Client 发送“访问令牌”access_token;

(9) Client 向 RS 提交 access_token, 请求资源授权;

(10) RS 为 Client 提供受保护的资源访问.

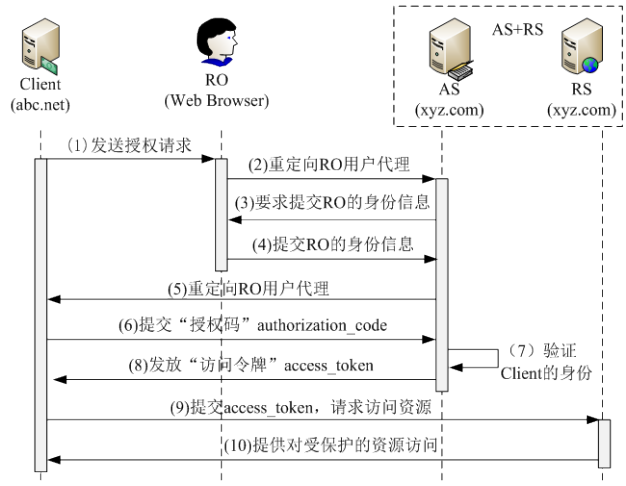

图 2 OAuth2.0 的跨域授权操作流程

在以上过程中, 当 Client 通过步骤(1)至步骤(8)获得对 RS 的 access_token 后, 在该 access_token 的有效期内, 用户在访问 RS 时只需要持该 access_token, 而不需要提交个人的身份信息, 保护了用户的隐私; 步骤(6)和步骤(7)中, 通过 authorizaton_code 换取 AS 的 access_token, 可避免各类网络攻击带来的安全风险, 并确保了 Client 身份的唯一性.

以上介绍的是两个安全域之间访问时，abc.net 域中的用户通过开放授权跨域访问 xyz.com 域中资源的具体实现方法. 其他安全域的加入方法与 abc.net 域的实现方法完全相同.

3.2 本方案的应用特点和优势

本方案的设计与实现，充分考虑到目前信息系统和资源整合过程中必须面对的实际问题，在云服务架构的支持下体现了既开放又继承的渐进式发展的思想，并将云计算所具有的弹性服务、按需服务、泛在接入及安全与隐私保护[2]得以较好地体现.

(1) 充分体现了云计算按需服务的特点. 按需服务是云计算的主要特征之一，也是实现细粒度授权操作的具体要求. 在如图 2 所示的实现方案中，xyz.com AS 可以根据 abc.net 中用户的不同需求(具体通过角色分配来实现)，有针对性的开放 xyz.com RS 上的资源;

(2) 充分体现了云计算的弹性服务特点. 云平台的开放性不仅仅反映在对接入资源的广泛吸纳性，而且体现在对服务规模的快速伸缩性. 在本方案中，通过对 RS 策略的管理，可以实现新域的随时接入或已有域的随时分离;

(3) 通过开放标准提供泛在服务和泛在接入能力. 随着电子商务、电子政务和高校数字化校园的快速发展，移动应用已经成为一种应用主流. OAuth2.0 协议的开放性，一方面可以方便地通过提供的安全 API 来实现与不同安全域之间更大范围的资源共享，另一方面允许笔记本电脑、智能手机、PAD 等移动终端随时随地访问云平台上的资源. 例如, Google 已通过 GData API 来支持 OAuth2.0.

(4) 提供了云环境开放架构下的安全及隐私保护功能. 本方案中，通过 OAuth2.0 的“访问令牌”避免了用户敏感信息的泄露，同时 OAuth2.0 还可以与 PKI(公钥基础设施)相结合，丰富认证功能.

另外，对于服务计费等功能需求，可通过与计费软件等专用软件对接来实现，本文不再单独介绍.

4 结语

云计算以开放授权方式打破了单一应用域的安全界线，出现了基于逻辑安全域的松耦合资源共享方式，在方便用户访问方式的同时降低了权限管理的代价. 开放授权的目的是允许 Web 应用用户离开原来的安全域到另一个安全域去访问资源，而无需再进行身份认证，成为 Web 站点之间自由移动和软件服务之间相连的有效工具，为应用程序之间提供了沟通和通信能力. 然而，云计算所具有的技术和非技术双重属性以及独有特征打破了传统单一域中的身份认证和资源授权模式，本文论述的基于 OAuth2.0 协议的开放授权技术和应用同样也是在云计算环境建设中的一个有益尝试，在取得已有良好应用的基础上，还将随着云计算的发展以及本研究项目的推进不断进行深入广泛的研究.

参考文献

1 Mell P, Grance T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011.

2 罗军舟,金嘉晖,宋爱波,等.云计算:体系架构与关键技术.通信学报,2011,7(32):3–31.

3 Cloud Security Alliance. Security Guidance for Critical Areas Offocus in Cloud Computing v2.1. 2009.

4 鲍美英,马礼,高玉斌.网格环境下授权策略的研究.微电子学与计算机,2010,27(3):43–46.

5 Raj H, Nathuji R, Singh A, et al. Resource management for isolation enhanced cloud services. Proc. of the 2009 ACM Workshop on Cloud Computing Security (CCSW'09). Chicago, USA, 2009. 77–84.

6 Roy I, Setty STV, Kilzer A, et al. Airavat: Security and privacy for MapReduce. Proc. of the 7th USENIX conference on Networked systems design and implementation (NSDI'10). USENIX Association Berkeley, CA, USA. 2010. 20.

7 Ristenpart T, Tromer E, Shacham H, et al. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Proc. of the 16th ACM Conference on Computer and Communications Security(CCS'09). ACM. 2009. 199–212.

8 冯登国,张敏,张妍,等.云计算安全研究.软件学报,2011,22(1):71–83.

9 Internet Engineering Task Force (IETF). The OAuth 2.0 Authorization Framework(RFC 6749). 2012.

10 Internet Engineering Task Force(IETF).OAuth 2.0 Dynamic Client Registration Core Protocol (draft-ietf-oauth-dyn-reg-16). 2014.

11 Internet Engineering Task Force(IETF).OAuth 2.0 Message Authentication Code(MAC) Tokens (draft-ietf-oauth-v2-http- mac-05). 2014.