

一种 Dubbo 框架的授权认证方案

范 迪,朱志祥

(西安邮电大学 物联网与两化融合研究院,陕西 西安 710061)

摘 要:为增强 Dubbo 分布式服务框架的访问安全性,避免服务消费过程中出现消费混乱或者数据被盗取的情况,将安全授权码应用到服务注册以及服务消费过程中,提出了一种新的访问控制方案。在 Dubbo 中引入授权认证中心,通过授权认证中心对服务提供方和服务消费方下发访问授权码,在服务注册阶段对服务提供者进行身份验证,服务提供者在服务被消费阶段对服务消费者进行身份验证,保证了数据交换过程中数据访问的安全性,有效地进行服务注册与服务消费的访问控制。授权认证中心同时依赖 Dubbo 构建成为分布式服务,与 Dubbo 框架本身进行深度融合,可以支撑高并发的授权码认证请求。该方案在 Dubbo 中增加授权认证中心,通过该模块下发和管理授权码,能够对注册授权和消费授权进行灵活管控,为 Dubbo 注册中心与服务提供方提供了更安全的访问控制,从而达到保护数据的目的。

关键词:Dubbo;授权认证;分布式服务框架;访问控制

中图分类号:TP311.1

文献标识码:A

文章编号:1673-629X(2017)11-0115-04

doi:10.3969/j.issn.1673-629X.2017.11.025

An Authorization Authentication Scheme for Dubbo Framework

FAN Di,ZHU Zhi-xiang

(Institute of IOT & IT-based Industrialization,Xi'an University of Posts and Telecommunications,
Xi'an 710061,China)

Abstract:In order to enhance the access security of Dubbo distributed service framework and avoid the circumstances of consumption confusion or data to be stolen in service consumption,the security authorization code is applies to service registration and service consumption and a new scheme of access control is proposed. Through the introduction of the authorized authentication center in Dubbo,the service provider and the consumer side can be issued security authorization code. According to that,service provider is authenticated in service registration and service consumer is authenticated by service provider in service consumption,which make sure the safety of data access in the process of data exchange,efficient access control of service registration and service consumption. In the meantime,the authorized authentication center establishes the distributed service by Dubbo and highly combines with Dubbo,which can support authentication request of authorization code with high concurrency. It adds the authorized authentication center in Dubbo to send and manage the authorization code which can conduct flexible control for registration authorization and consumption authorization,providing the safer access control for Dubbo registration center and service provider and reaching the purpose of data protection.

Key words:Dubbo;authorization authentication;distributed service framework;access control

0 引 言

随着互联网的发展,网站应用的规模不断扩大,分布式服务架构以及流动计算架构势在必行^[1]。Dubbo 是一个分布式服务框架以及 SOA 治理方案,致力于提供高性能和透明化的 RPC 远程服务调用方案,是阿里巴巴 SOA 服务化治理方案的核心框架,每天为 2 000+ 个服务提供 3 000 000 000+次访问量支持,并广泛应用

于阿里巴巴集团的各成员站点。Dubbo 自开源后已经被很多非阿里系公司使用^[2-3]。

数据作为信息时代最重要的资产^[4],在互联网时代也被作为商品进行消费,所以在跨行业、跨部门之间建设数据交换共享服务,将本行业数据作为一种商品提供给需要的行业部门,减少因重复建设造成的社会资源浪费,通过优势资源为自身服务并节省成本,集中

收稿日期:2016-11-20

修回日期:2017-03-15

网络出版时间:2017-07-19

基金项目:基于大数据的陕西省政府和社会信息资源开放共享策略研究项目(2016KRM047);陕西省科技统筹创新工程计划项目(2016KTTSGY01-01)。

作者简介:范 迪(1993-),女,硕士,研究方向为大数据处理与高性能计算;朱志祥,教授,博士,研究方向为信息安全。

网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20170719.1112.078.html

精力提高自身核心竞争力,必然是互联网社会分工的趋势^[5-6]。利用 Dubbo 分布式服务框架构建大型数据交换平台,不仅能够简化应用系统开发,而且可以灵活扩展服务,是建设数据交换中心的一种可行方案。由于 Dubbo 分布式服务框架的服务治理功能依赖于服务注册中心^[7-8],而服务注册中心并没有对服务注册过程进行严格的身份验证,同时,服务消费过程是消费者对提供者的直接访问,而提供者也没有对消费者身份进行验证,因此对于数据交换来说,造成了很大的安全隐患。

授权认证方案通过引入授权认证中心模块进行服务支持,为利用 Dubbo 分布式服务框架构建的数据交换平台提供一种访问控制方法,对服务注册和服务消费进行严格的身份认证和访问控制。

1 系统架构设计

系统在 Dubbo 框架中引入管理中心、授权认证中心两个新模块,结合框架原有的注册中心、服务提供者、服务消费者共同构成完整的系统^[9-10],系统架构如图 1 所示。

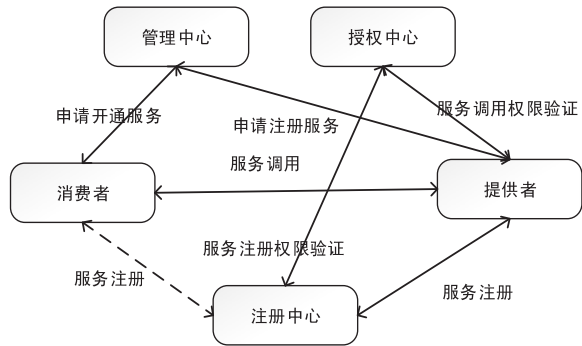


图 1 系统整体架构

管理中心整合了授权认证中心和注册中心的功能,实现服务目录和服务治理的功能。授权认证中心包括两部分工作:根据服务名生成授权码,通过授权码对服务进行授权,授权包括服务注册授权和服务消费授权;验证提供授权码的服务身份,通过对授权码进行多项验证,检查发起请求的服务是否经过授权。系统要求注册中心和服务提供者在响应服务之前向授权认证中心验证请求中携带的授权码信息。

2 授权码

授权认证中心采用 AppId(应用标识)和 Secret-Key(访问密钥)作为一组授权码进行授权^[11],授权码除了有启用和禁用的状态限制外,还有使用次数和有效时间作为限制。使用次数和有效时间是管理中心对服务进行授权时指定的,和状态限制一样可以动态修改^[12]。万方数据

3 授权认证过程

授权和认证涉及两个过程:服务注册和服务消费。服务注册是服务消费的前提,注册到注册中心的服务会通过管理中心同步到服务目录中,服务消费者才可以在服务目录中进行申请开通服务,开通服务后可对服务进行消费。

服务注册授权认证过程如图 2 所示。

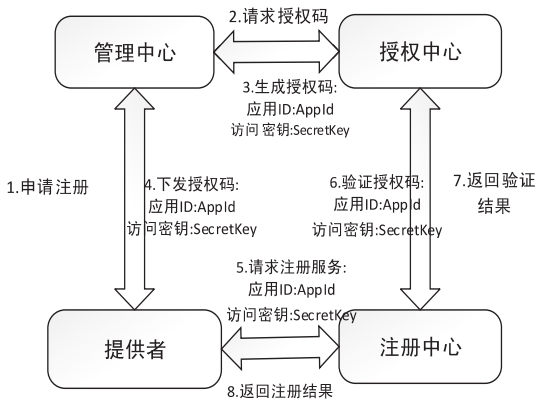


图 2 服务注册授权认证流程

服务提供者首先需在管理中心申请注册服务,管理中心会对服务申请进行审核授权,若通过审核,则向授权认证中心请求授权码,授权认证中心生成授权码,返回给管理中心,由管理中心下发授权码给服务提供者,此时提供者可携带该授权码向注册中心请求注册服务,注册中心向授权认证中心验证此授权码是否合法。服务注册授权不涉及调用次数和有效时间的限制,只受状态码的影响。注册验证过程如下:

(1) 注册中心接收到服务提供者的注册请求,获取请求中携带的授权码信息,向授权认证中心发起注册认证请求;

(2) 授权认证中心接收到注册验证请求,根据 AppId 查询授权码是否存在,若不存在,返回 failed 信息,错误描述信息为“授权码信息不存在,请向管理中心申请注册授权码”;

(3) 验证授权码 SecretKey, SecretKey 不匹配时返回 failed 信息,错误描述信息为“授权码错误”,Secret-Key 验证匹配继续下一步认证;

(4) 检查授权码状态,状态为“禁用”时返回 failed 信息,错误描述信息为“授权码已被禁用”,状态为“启用”时返回 success 信息,成功描述信息为“身份认证通过”;

(5) 注册中心根据授权认证中心的返回信息进行下一步处理,注册验证通过则将服务注册到注册中心,注册验证失败直接向服务提供者返回注册失败信息。

服务消费授权认证过程如图 3 所示。

服务消费者首先需向管理中心申请开通服务。与服务注册不同,服务消费者需要在服务目录中对需开

通的服务进行申请,由管理中心进行审核,审核通过后向服务消费者下发对应需要开通服务的授权码 (AppId 和 SecretKey),服务消费者调用服务时需要向服务提供者提供服务授权码,提供者接收到消费者的请求后先对授权码进行验证,由提供者向授权认证中心发起身份验证请求,验证通过后再对请求进行服务响应,每成功响应一次,需要向授权认证中心反馈调用结果,对服务调用次数加 1。服务过程如下:

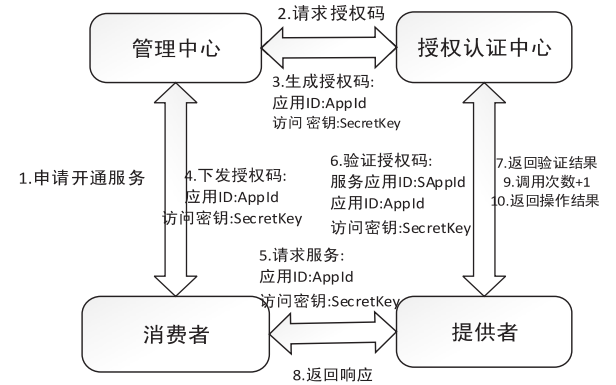


图 3 服务消费授权认证流程

- (1) 服务提供者接收到服务消费者的消费请求,从消费请求中获取消费授权码,并向授权认证中心发起消费认证请求;
- (2) 授权认证中心接收到消费认证请求,首先对发起请求的服务提供者状态进行验证,如果服务提供者已被管理中心禁用,则返回 failed 信息,错误描述信息为“服务提供者已被禁用”,如果服务提供者状态正常,则继续下一步认证;
- (3) 根据 AppId 查询授权码是否存在,若不存在,返回 failed 信息,错误描述信息为“授权码信息不存在,请向管理中心申请消费授权码”;
- (4) 验证授权码 SecretKey,SecretKey 不匹配时返回 failed 信息,错误描述信息为“授权码错误”,SecretKey 验证匹配则继续下一步认证;
- (5) 检查授权码状态,当状态为“禁用”时返回 failed 信息,错误描述信息为“授权码已被禁用”,当状态为“启用”时继续下一步认证;
- (6) 验证授权码有效时间,若超出有效时间则返回 failed 信息,错误描述信息为“授权码已超出有效时间”,若在有效期内,则继续下一步认证;
- (7) 验证授权码调用次数,若达到指定的调用次数时返回 failed 信息,错误描述信息为“授权码调用次数已达到上限”,若未达到指定的调用次数,则返回 success 信息,成功描述信息为“身份认证通过”;
- (8) 服务提供者根据授权认证中心的反馈进行服务响应,若认证失败,直接返回认证失败信息,若认证通过,则执行对应的服务代码进行服务响应;

- (9) 服务响应完成后,向授权认证中心发起消费者调用次数更新请求,将调用次数加 1。
- 4 实验验证
- 通过对服务注册和服务消费两个过程的授权码生成并下发和授权码认证进行实验,先通过管理中心向授权认证中心为服务提供者请求生成一对注册授权码,由服务提供者携带注册授权码向注册中心进行服务注册。注册过程会对授权码进行三个阶段验证,验证参数与结果如下:
- 生成的注册授权码:
- AppId:
- 32a04c86f200480396a0d5a9b0257714
- SecretKey:
- 14f6a61132134de2b210801a5ef6e
- 验证 1 参数条件,AppId 错误,SecretKey 正确,状态启用。
- AppId:
- 5ceaad9bba9143afad9f4b2450a30d52
- SecretKey:
- 14f6a61132134de2b210801a5ef6e
- 返回值:{"status": "failed", "message": "授权码信息不存在,请向管理中心申请注册授权码"}。
- 验证 2 参数条件,AppId 正确,SecretKey 错误,状态启用。
- AppId:
- 32a04c86f200480396a0d5a9b0257714
- SecretKey:
- 779eb55b9a154442bba8b0d8f87e7
- 返回值:{"status": "failed", "message": "授权码错误"}。
- 验证 3 参数条件,AppId 正确,SecretKey 正确,状态禁用。
- AppId:
- 5ceaad9bba9143afad9f4b2450a30d52
- SecretKey:
- 14f6a61132134de2b210801a5ef6e
- 返回值:{"status": "failed", "message": "授权码已被禁用"}。
- 验证 4 参数条件,AppId 正确,SecretKey 正确,状态启用。
- AppId:
- 5ceaad9bba9143afad9f4b2450a30d52
- SecretKey:
- 14f6a61132134de2b210801a5ef6e
- 返回值:{"status": "success", "message": "身份认证通过"}。

认证通过”}。

服务提供者注册成功后,服务消费者在服务目录中对已上线的服务进行申请开通,由管理中心向授权认证中心请求消费授权码并下发给服务消费者,服务消费者携带消费授权码向服务提供者进行服务请求。服务消费过程会对授权码进行六个阶段验证,验证结果如下:

生成的消费授权码:
AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
验证 1 参数条件,服务提供者被禁用,AppId 正确,SecretKey 正确,状态启用,调用次数未达到限制,未过期。
AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
返回值:{“status”:“failed”,“message”:“服务提供者已被禁用”}。

验证 2 参数条件,服务提供者被启用,AppId 错误,SecretKey 正确,状态启用,调用次数未达到限制,未过期。

AppId:
3b7375625daa47d6a609413b29f1328d
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
返回值:{“status”:“failed”,“message”:“授权码信息不存在,请向管理中心申请注册授权码”}。

验证 3 参数条件,服务提供者被启用,AppId 正确,SecretKey 错误,状态启用,未过期,调用次数未达到限制。

AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
a3191d1c17bd4bba8fad8f5452917
返回值:{“status”:“failed”,“message”:“授权码错误”}。

验证 4 参数条件,服务提供者被启用,AppId 正确,SecretKey 正确,状态禁用,未过期,调用次数未达到限制。

AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b

返回值:{“status”:“failed”,“message”:“授权码已被禁用”}。

验证 5 参数条件,服务提供者被启用,AppId 正确,SecretKey 正确,状态启用,已过期,调用次数未达到限制。

AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
返回值:{“status”:“failed”,“message”:“授权码已超出有效时间”}。

验证 6 参数条件,服务提供者被启用,AppId 正确,SecretKey 正确,状态启用,未过期,调用次数达到限制。

AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
返回值:{“status”:“failed”,“message”:“授权码调用次数已达到上限”}。

验证 7 参数条件,服务提供者被启用,AppId 正确,SecretKey 正确,状态启用,未过期,调用次数未达到限制。

AppId:
f9c4cc018be648d2a68247dfcc3a1de0
SecretKey:
da2647f54c04aeb8244bc5333b29e1b
返回值:{“status”:“success”,“message”:“身份认证通过”}。

5 结束语

授权认证中心能够对服务注册和服务消费生成对应的授权码,并在授权码验证过程中对可能出现的各种情况进行正确的判断并返回准确的验证信息。

在 Dubbo 中引入授权认证中心,能够对服务提供者在分布式应用中进行接入控制,同时对服务消费过程进行权限控制,有效保护服务提供者的资源并对消费者行为进行合理的统计和控制。

参考文献:

[1] Yanjun. Dubbo 架构设计详解[EB/OL]. (2013-09-03) [2016-11-03]. <http://shiyanyun.cn/archives/325.html>.
[2] 丁振凡. Spring REST 风格 Web 服务的 Json 消息封装及解析研究[J]. 智能计算机与应用,2012,2(2):9-10.
[3] 王元卓,靳小龙,程学旗. 网络大数据:现状与展望[J]. 计

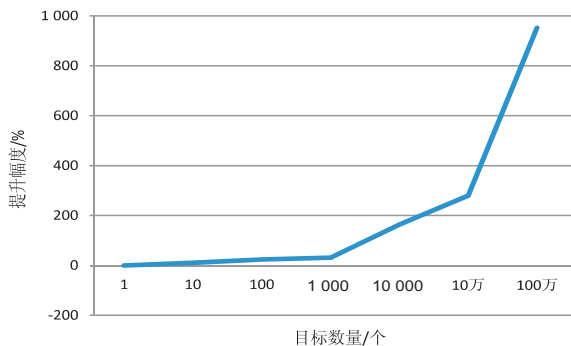


图 3 文中方法与二分法针对不同目标数量的效率提升幅度

这也和之前的预期是一致的,充分证明了提出方法的有效性和优越性。

4 结束语

GPU 作为高速并行运算设备,在各类口令暴力破解中的作用日益凸显。基于目标映射,设计了一种在 GPU 上进行的解密目标快速比对方法,使得暴力破解的效率显著提升。同时,还实现了基于经典二分比对法和基于该方法的 MD5 暴力破解程序,充分验证了提出的 GPU 快速比对法对暴力破解效率的有效提升。

实验结果表明,使用二分法比对的 MD5 暴力破解算法,随着解密目标数量的增加,效率逐渐降低。在相同的实验环境下,使用文中的目标快速比对算法,效率提升明显,且目标数量越多,提升效率越明显。

文中方法可以应用于各种散列类型的解密程序中,针对不同目标类型仅需修改方法中部分参数即可,使用十分便捷。针对散列类型的暴力破解尤其是针对本身加密速度很快的散列类型有着极大的提升作用。

参考文献:

[1] Forouzan B A. 密码学与网络安全[M]. 马振哈,贾军保,

译. 北京:清华大学出版社,2009.

- [2] 翁捷,吴强,杨灿群. 基于 OpenCL 的 MD5 破解算法[J]. 计算机工程,2011,37(4):119-121.
- [3] Chen R,Zhang Y,Zhang J, et al. Design and optimizations of the MD5 crypt cracking algorithm based on CUDA[C]//International conference on cloud computing. [s. l.]: Springer International Publishing,2015:155-164.
- [4] 张丽丽,张玉清. 基于分布式计算的暴力破解分组密码算法[J]. 计算机工程,2008,34(13):121-123.
- [5] 石志才. 异构平台上协同计算的相关研究[D]. 长沙:国防科学技术大学,2011.
- [6] Vu A D,Han J I,Nguyen H A, et al. A homogeneous parallel brute force cracking algorithm on the GPU[C]//International conference on ICT convergence. [s. l.]: IEEE,2011:561-564.
- [7] Niewiadomska-Szynkiewicz E,Marks M,Jantura J, et al. Comparative study of massively parallel cryptanalysis and cryptography on CPU-GPU cluster[C]//Military communications and information systems conference. [s. l.]:[s. n.],2013:1-8.
- [8] 乐德广,常晋义,刘祥南,等. 基于 GPU 的 MD5 高速解密算法的实现[J]. 计算机工程,2010,36(11):154-155.
- [9] Wang F,Yang C,Wu Q, et al. Constant memory optimizations in MD5 crypt cracking algorithm on GPU-accelerated super-computer using CUDA[C]//International conference on computer science & education. [s. l.]:[s. n.],2012:638-642.
- [10] 谢鑫君,罗顺,杨士华. 基于口令自生成的 GPU 暴力破解优化技术[J]. 信息安全与通信保密,2013(3):82-84.
- [11] 张奇. 基于 CUDA 架构的 MD5 并行破解算法设计与实现[D]. 成都:电子科技大学,2012.
- [12] 陈钢,吴百锋. 面向 OpenCL 模型的 GPU 性能优化[J]. 计算机辅助设计与图形学学报,2011,23(4):571-581.
- [13] 张润梅,王霄. 基于 CUDA 架构的 MD5 破解方法研究[J]. 计算机科学,2011,38(2):302-304.
- [14] 于飞,吉庆兵,罗顺,等. GPU 计算及其在密码分析中的应用[J]. 信息安全与通信保密,2012(12):98-100.

(上接第 118 页)

计算机学报,2013,36(6):1125-1138.

- [4] 王涛. 数据共享与数据交换系统的设计与实现[D]. 大连:大连理工大学,2015.
- [5] 曾一,袁纲,张元平,等. 基于 Web 服务的电子政务数据交换中心的设计和实现[J]. 计算机科学,2007,34(11):98-102.
- [6] Sheu R K,Yuan S M,Lo W T. MEDEA-a model for the event-based data exchange architecture[C]//Proceedings of the seventh international conference on parallel and distributed systems. Washington,DC:IEEE,2000:88.
- [7] 时子庆,刘金兰,谭晓华. 基于 OAuth2.0 的认证授权技术[J]. 计算机系统应用,2012,21(3):260-264.
- [8] 王力军,陈为数据,杨小军. OAuth2.0 协议认证授权实现方

案研究[J]. 电脑编程技巧与维护,2015(10):21-22.

- [9] Sprott D,Wilkes L. Understanding service-oriented architecture,CBDI[EB/OL]. 2004. <http://www.microsoft.com/china/MSDN/library/architecture/>.
- [10] Carey P F,Gleason B W. Solving the integration issue-service-oriented architecture[EB/OL]. 2006. <http://www.zdnet.co.uk/tsearch/Service-Oriented+Architecture.htm>.
- [11] 史新,乔晓东,张志平,等. 汉语科技词系统的 Web 服务研究与实现[J]. 现代图书情报技术,2008(12):37-42.
- [12] Barry D K. Service-oriented architecture (SOA) definition[EB/OL]. 2011-01-28. http://www.service-architecture.com/web-services/articles/service-oriented_architecture_soa_definition.html.