基于RBAC框架实现ABAC

何新新[1, 2]，纪阳[1, 2]

[1] 北京邮电大学移动生活与新媒体实验室，北京100876

[2] 北京邮电大学泛网无线通信教育部重点实验室，北京 100876

摘要：基于属性的访问控制ABAC可以实现细粒度的访问控制，但是到目前为止，并没有一个统一的实现架构。传统的RABC通过“角色”建立起用户和资源的关系，极大简化了权限的分配问题，并且RBAC已有成熟的实现架构。本文提出一种在RBAC的架构中实现ABAC的方法，通过分类算法充分结合两者的优势。

关键词：ABAC；RBAC；分类

中图分类号： TP311

The achievement of ABAC based on the framework of RBAC

He Xin-xin[1, 2], Ji Yang[1, 2]

[1] Beijing University of Posts and Telecommunications Mobile Life and New Media Lab, Beijing 100876

[2] Beijing University of Posts and Telecommunications Key Laboratory of Universal Wireless Communications,Ministry of Education, Beijing 100876

Abstract: ABAC (attribute-based access control) can be achieved fine-grained access control, but so far, no one unified implementation architecture. Traditional RABC through ”role” to establish the relationship between users and resources, greatly simplifying the distribution of authority, and RBAC has a mature implementation architecture. This paper presents a solution to achieve ABAC in RBAC architecture, use classification algorithm, fully integrate the advantages of both.

Key words: ABAC; RBAC; Classification

0 引言

基于属性的访问控制(Attribute Based Access Control, ABAC)能解决复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题。传统访问控制大多依据主体和资源的标识制定访问控制策略，而ABAC 中充分考虑主体、资源和访问所处环境的属性信息来描述策略，策略的表达能力更强、灵活性更大。

基金项目： 基于Web的无线泛在业务环境体系架构、关键技术研究与演示验证(2012ZX03005008-001)

作者简介： 何新新（1989-），男，硕士，主要研究方向：网络安全,Email:hexinxin1202@gmail.com。通信作者：纪阳（1972-），男，教授，主要研究方向：宽带移动通信新技术研究，移动互联网业务与应用、泛在网技术、Livinglab创新模式,Email:jiyang@bupt.edu.cn。

A.H. Karp, H. Haury, and M.H. Davis在文章[1]中提出，基于属性的访问控制（ABAC）利用属性和规则取代RBAC或使其更加简单、灵活。但是，到目前为止，ABAC没有其共识的统一架构。

RBAC虽然没有实现动态分配权限和细粒度的访问控制，但是，RBAC通过“角色”建立起用户和资源的关系，极大简化了权限的分配问题，而且RBAC已有成熟的实现架构。

本文提出了一种在RBAC框架中实现ABAC的方案。考虑到ABAC和RBAC的各自优势，本文提出了一种结合两者优势的ABAC实现方案，该方案的核心是“分类”，即根据用户（资源）属性判断用户（资源）属于哪些用户（资源）属性类。

1 ABAC的实现

根据用户和资源的属性进行分类，是在RBAC中实现ABAC的关键。本文提出了一种在RBAC中实现ABAC的方法，根据用户和资源的属性，判断用户和资源属性哪些用户和资源属性类，通过用户属性类和资源属性类建立用户和资源的关系，并分配一个属性类的classId，此属性类classId相当与传统RBAC中的role，与具体的权限对应，这样讲属性与具体的操作权限通过建立映射，方便权限的而管理。根据ABAC的策略：具有属性“CS”的用户对具有属性“CT”的资源具有“P”操作权限，可以抽象为属性权限矩阵CS-CT-P和属性类矩阵C，CS为用户属性类，CT为资源属性类。

$$\mathbf{CS-CT-P}=\begin{pmatrix} & CT_1 & CT_2 & \dots \\ CS_1 & P_{11} & P_{12} & \dots \\ CS_2 & P_{21} & P_{22} & \dots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

$$\mathbf{C}=\begin{pmatrix} C_{11} & C_{21} & \dots \\ C_{12} & C_{22} & \dots \\ \dots & \dots & \dots \\ C_{1J} & C_{2J} & \dots \end{pmatrix} \quad C_{ij}=\begin{cases} 1 & \text{要求的用户属性} \\ 0 & \text{无要求} \end{cases}$$

根据C矩阵可以断定用户（资源）属于哪些用户（资源）属性类。例如：用户Ui的

$$CS=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

表示用户Ui属于用户属性类1和2. 通过引入属性类classId方便的将用户、资源和权限建立起映射关系，但是，ABAC中的权限判断的流程和数据库的设计与RBAC中有所区别，下面介绍ABAC中的权限判断具体流程和数据库的设计。

1.1 ABAC权限判断

ABAC中权限判断的核心思路是：通过用户和资源的ID得到用户和资源的属性，然后通过分类算法确定用户属性类和资源属性类，通过查找其具体的操作权限。

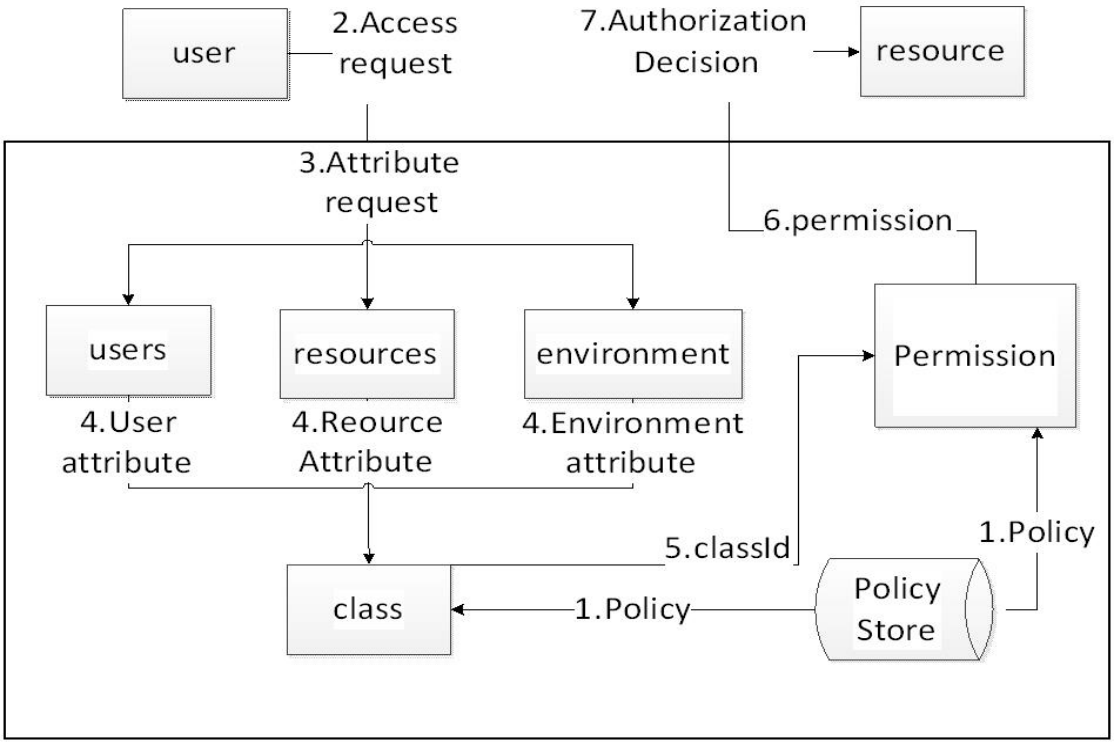

图 1: ABAC流程图

定义：

userId：用户身份的唯一凭证，正如新浪微博一样，每个用户都有唯一的一个ID，此ID是用户的唯一凭证。userClass：用户属性类（用户属性类由策略决定）。resourceId：资源的唯一凭证。resourceClass：资源属性类（资源属性类由策略决定）。classId：代表属于某用户属性类的用户对属于某资源属性类的资源有什么样的操作权限。(classId根据策略库中的策略定义)。每个classId代表一种操作权限，比如：1111 代表POST / GET / PUT / DELETE。

(1) 从Policy Store获取相关策略，转换并保存。(2) 访问请求者提出访问请求，ABAC拦截请求消息。(3) ABAC获取、、环境信息，向Users、Resources、environment发送属性请求。(4) Users、Resources、environment 根据传递的用户和资源id和环境信息，将相关的属性信息发送给class。(5) Class根据用户属性资源属性环境属性对其分类得到、，并将发送给Permission。(6) Permission根据，获得映射的操作权限。(7) 如果访问请求被允许，则Permission转发访问请求，并将相应的响应消息回送给访问请求者。

1.2 数据库的设计

ABAC的数据库根据RBAC的数据库进行设计，最大的不同是ABAC数据库要考虑用户资源的属性信息以及属性的分类算法。

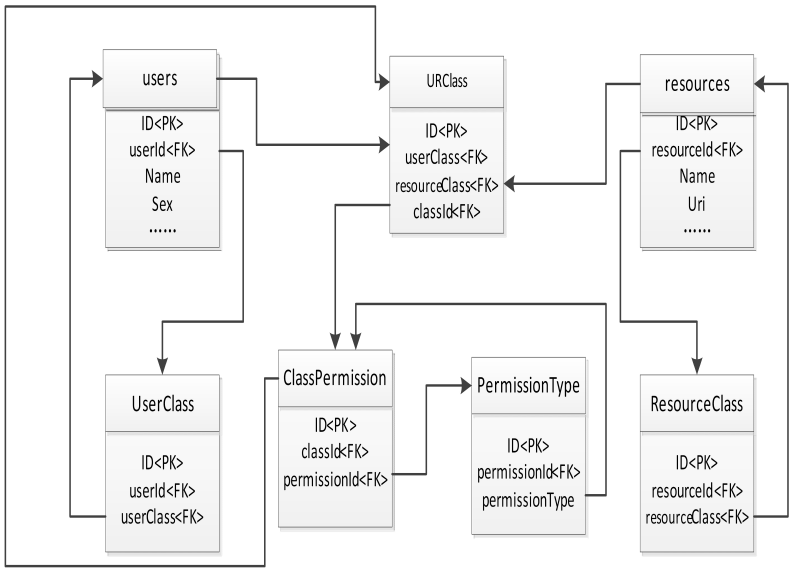

图 2: ABAC数据库设计

数据库中一共7张表，users、resources、UserClass、ResourceClass、URClass、ClassPermission、PermissionType。users表存储用户属性信息。Resources表存储资源属性信息。UserClass表存储用户属性类信息，通过userId建立与用户的联系。ResourceClass表存储资源属性类信息，通过resourceId建立与资源的联系。URClass表通过userClass和resourceClass建立用户和资源的联系。ClassPermission表存储属性类对与操作权限的联系，通过classId建立联系。PermissionType表存储具体的操作权限，共16种，通过permissionId与classId建立联系。

2 系统评估

从理论上分析ABAC系统的性能，用户数目和资源数目理论上对ABAC系统的性能影响不大。本文对RBAC和RBAC框架中实现的ABAC系统进行了仿真测试，通过测试结果可以得出结论：ABAC在不增加系统负担的情况下，充分考虑属性信息，实现动态分配权限和细粒度的访问控制。

图3为在用户资源数目相同，RBAC的角色数与ABAC的classId相同的情况下，测得的平均时延。系统的性能理论上会随着并发数的增加而变差，即时延会变大。由上图可以看出，系统的整体性能与理论分析一致。在RBAC框架中实现的ABAC系统，虽然整体性能与RBAC类似，但是随着并发数及用户数的增多，ABAC的性能优于原RBAC的性能。

图4为ABAC中资源数目和用户数目增加一倍的情况下时延对比，由上图可以看出，资源数目和用户数目的增多对ABAC系统性能的影响不大，这与理论分析得出的结论一致。

由测试结果可以看出，RBAC框架中实现的ABAC系统，在没有增加时延的情况下，优化了整个访问控制系统，说明此方案是可行的。

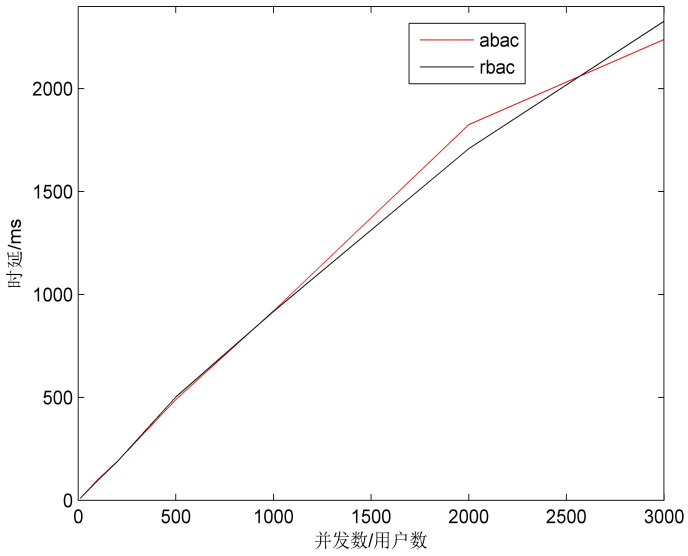

图 3: abac与rbac时延对比

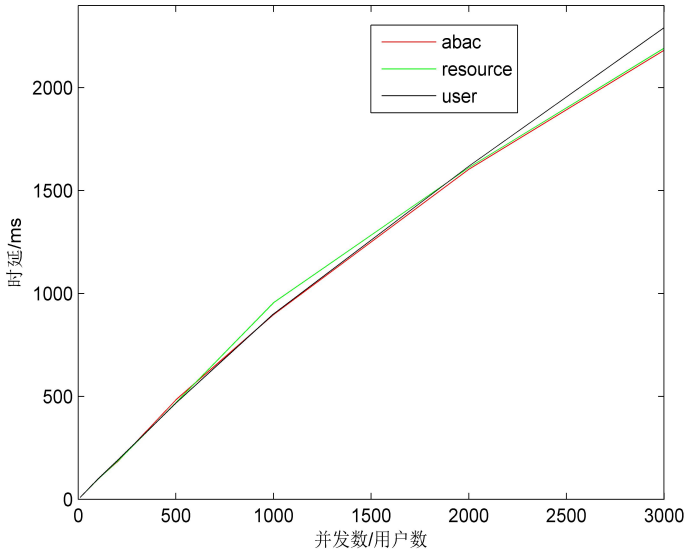

图 4: abac中时延对比

3 相关工作

基于角色的访问控制[2, 3](RBAC) ,为信息安全提供了一种流行的模式，有助于降低安全管理的复杂性和支持审查分配给用户的权限。文章[3]给出了RBAC的模型。当动态的属性可能成为决定用户权限的因素时，基于属性的访问控制（ABAC）被提出。

基于属性的访问控制（ABAC）中充分考虑主体、资源和访问所处环境的属性信息来描述策略，策略的表达能力更强、灵活性更大[4]。

虽然基于属性的访问控制（ABAC）没有统一共识的模型，但是根据属性判断访问权限的方法比基于角色的访问控制（RBAC）更加灵活[1]。

针对RBAC与ABAC的缺点：RBAC设计困难但是方便权限的管理；ABAC设计方便但是存在改变权限的问题。文章[5]提出了3种实现在RBAC引入属性的方法, Dynamic roles, Attribute-centric, Role-centric.一个纯粹的RBAC系统不能够支持动态的属性如时间，这些属性有可能成为决定用户权限的因素。

文章[6]提出了一种给用户动态分配角色的模型。文中提出了一种表达属性的方法，用户的属性通过属性表达式来定义。为了根据用户属性匹配规则，他们提出了一种分层次的思想，比如age role: child, age role: juvenile, age role: adolescent, age role:adult.

为了适应web服务，文章[7, 8, 9]针对web环境，分别从理论和应用两方面研究设计ABAC模型，并提出了针对web服务ABAC安全架构。

文章[10]分析了现有的访问控制系统的不足，提出了一种基于属性和角色的访问控制(ARBAC，attribute and role based access control)，根据用户的属性建立用户与role的映射。

4 结论

本文给出了一种在RBAC架构中实现ABAC的方法，该方法的关键在于根据属性对用户和资源进行分类。目前为止，ABAC没有共识的架构模型，应用RBAC成熟的Spring架构实现ABAC可以避免一些安全问题。由测试结果可知，虽然该方案的测试时延与RBAC的时延相差甚小，但是它的灵活性和可扩展性优于RBAC。

本文只是提出了一种ABAC的实现方法，没有考虑ABAC中必须的属性权威、策略冲突等问题，这些都是该方法需要完善的地方。

参考文献（References）

[1] Karp A H, Haury H, Davis M H. From ABAC to ZBAC: the evolution of access control models[J]. Hewlett-Packard Development Company, LP, 2009:21.

[2] Ferraiolo D F, Kuhn D R. Role-based access controls[J]. arXiv preprint arXiv:0903.2171, 2009: 554-563.

[3] Sandhu R S. Role-based access control[J]. Advances in computers, 1998, 46: 237-286.

[4] 李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型[J]. 通信学报, 2008, 29(4): 90-98.

[5] Kuhn D R, Coyne E J, Weil T R. Adding attributes to role-based access control[J]. IEEE Computer, 2010, 43(6): 79-81.

[6] Al-Kahtani M A, Sandhu R. A model for attribute-based user-role assignment[A]. Al-Kahtani M A. 18th Annual Computer Security Applications Conference (ACSAC 2002)[C]. USA:The Printing House ,2002:353 - 362.

[7] Yuan E, Tong J. Attributed based access control (ABAC) for web services[A]. Yuan E. 2005 IEEE International Conference on Web Service[C]. Los Alamitos, CA 90720-1314,2005:25.

[8] Shen H, Hong F. An attribute-based access control model for web services[A]. Shen H. Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies[C]. Los Alamitos, CA 90720-1314, 2006:74-79.

[9] 夏春涛, 杨艳丽, 曹利峰. 基于ABAC 的Web Services 访问控制研究[J]. 计算机应用与软件, 2012, 29(2): 83-85.

[10] Liu M, Guo H Q, Su J D. An attribute and role based access control model for Web services[A]. Liu M. 2005 International Conference on Machine Learning and Cybernetics[C]. China: Guangzhou 2005: 1302 - 1306 Vol. 2.