基于表单访问权限控制策略

吴承来[1],周传华[1],周家亿[2]
(1. 安徽工业大学 管理科学与工程学院,安徽 马鞍山 243032;
2. 东南大学 计算机科学与工程学院,江苏 南京 211189)

摘 要:为解决权限控制交互性问题,在属性访问控制的基础上提出了一种基于表单访问权限控制策略。策略引入表单实体,使用表单和属性映射表实现了用户界面和数据属性的双向权限控制,在保留了属性访问控制安全性和灵活性的基础上,进一步提升了权限控制的用户交互性,改进的权限管理模型更适用于工程应用中权限控制的实现。最后,用图灵机对策略进行安全分析,从理论上保证该策略的安全可靠性。原型系统实现基于面向对象(OO)和面向切面编程(AOP)思想以及 Java 标签和 Ajax 技术,实现了权限控制对业务系统的低侵入性和松散耦合,加强了系统的可维护性和可重用性,并且使得该策略的有效性和灵活性得到了验证。

关键词:权限管理模型;表单控制;控制粒度;映射表;安全分析;图灵机
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2016)02-0035-04
doi:10.3969/j.issn.1673-629X.2016.02.008

Form Based Access Control Strategy

WU Cheng-lai[1],ZHOU Chuan-hua[1],ZHOU Jia-yi[2]
(1. School of Management Science and Engineering,Anhui University of Technology,Ma'anshan 243032,China;
2. School of Computer Science and Engineering,Southeast University,Nanjing 211189,China)

Abstract:To solve the problem of user interactiveness,based on attribute access control,a form based access control strategy was proposed. The form is introduced into the strategy,which uses the form and attribute mapping table to achieve the two-way access control of user interface and data layer. The strategy ensures the safety and flexibility of attribute access control,enhancing user interactiveness of access control further. Improved access control model is applied more strongly in access control in engineering application. Eventually,the reliability of the strategy is guaranteed in theory by analyzing its safety with turing machine. Based on Object Oriented (OO) and Aspect Oriented Programming (AOP),Java Tag and Ajax technology,the prototype system,to the business system,implements low invasive and loose coupling of the access control,strengthening its the maintainability and reusability. Meanwhile,the effectiveness and flexibility of the strategy are verified.

Key words:privilege management model;form based access control;granularity of access control;mapping table;safety analysis;turing machine

1 概 述

随着全球经济一体化步伐的加快,信息技术在各个领域应用的深度和广度不断拓展,使得信息系统的集成性和复杂性不断加大,而且对信息系统的交互性和用户体验要求越来越高。传统基于 RBAC 的权限控制模型往往不能有效解决全球一体化背景下信息系统越来越复杂的权限控制需求。当前信息系统权限控制主要面临以下三个问题和挑战:分布式和跨域环境下的权限控制问题,基于时空上下文的权限控制问题,权限的控制粒度和权限控制的用户交互性问题[1-2]。

针对上述权限控制问题,学术界和工程界提出了相应的解决方案。

在分布式和跨域环境下的权限控制方面,Freudenthal 等提出了分布式角色访问控制模型(Distributed Role-Based Access Control,DRBAC)[3]。该模型利用 PKI 识别操作实体的身份和验证委托证书,在跨多个管理域的动态协作环境中实现了资源的访问控制;Liu 等针对分布式协同操作环境中基于角色的访

收稿日期:2015-05-07 **修回日期**:2015-08-14 **网络出版时间**:2016-01-26
基金项目:国家自然科学基金面上项目(71172219);安徽省教育厅重大计划项目(ZD200904))
作者简介:吴承来(1990-),男,硕士研究生,CCF 会员,研究方向为软件工程、信息安全;周传华,教授,研究方向为信息安全、机器学习。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160126.1517.022.html

问控制在利用角色映射的方式时可能存在的安全问题,提出了一种适用于分布式协同操作环境的 RBAC 模型(Role-Based Access Control model for Distributed Cooperation environment,RBAC-DC)[4]。

随着移动互联网的发展,出现了很多基于位置的服务和应用软件,传统的权限控制模型不能很好地解决基于空间上下文的权限控制,所以有学者提出了基于时空上下文的权限控制模型。Ray 等提出了一个位置感知的访问控制模型(Location-aware Role Based Access Control,LRBAC),通过引入空间角色的概念将空间上下文集成到角色中,可根据用户的当前位置来判断会话中哪些角色是有效的[5-6];张颖君等在访问控制中同时整合了时间和空间因素,提出了一种基于尺度的时空 RBAC 模型[7-8]。

在权限的控制粒度方面,熊智提出了一种云储存环境下的基于属性的权限控制方案[9],采用字典变量表示主客体等实体,为云环境下文件提供了一种高效的权限控制方法;赵卫东和李阳提出了一种细粒度的权限控制模型[10-11],李阳在他的论文中提出了一种基于 UCON 的属性访问控制模型(attribute based access control model),将属性和角色授权委托引入了控制模型,细化了模型的控制粒度,但是该模型只能对数据属性进行权限控制,没有考虑对用户界面的控制,基于该模型实现的权限系统用户交互性较差。

在工程界,中间件提供商将权限控制的理念抽取出来,在 RBAC 模型的基础上单独形成一套权限系统,解决需要权限控制的系统需求,增强了用户体验。但用它来控制权限的系统,必须在界面上统一风格,对业务系统存在很强的侵入性,而且只是实现了对权限的功能级控制,没有实现对数据属性和表单的权限控制。Spring Security 和 Apache Shiro 都基于 RBAC 提供了一套底层的权限管理方案[12-13],简化了权限管理的实现过程。但这些方案都是对 RBAC 模型的部分封装和实现。RABC96 元素关系图如图 1 所示。

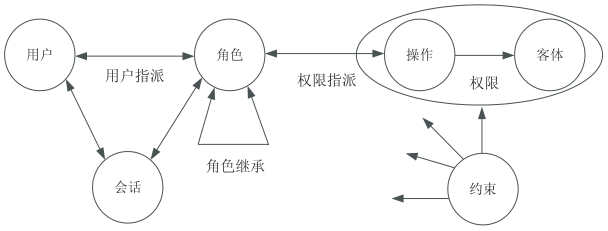

图 1 RABC96 元素关系图

学术界和工程界越来越关注权限系统的安全性和用户交互性问题。文中在这种背景下,旨在提出一种安全可靠且有良好用户交互性的权限控制策略。表单访问权限控制在策略中引入了表单实体,从模型组件层扩展了基于属性的访问控制模型,该策略具有了对表单权限控制的能力,策略中采用表单和属性映射表,实现了用户接口层和数据层的双向权限控制,在保证安全的前提下,增强了用户交互性,且更易于工程实现。在该策略的实现过程中,采用纯面向对象和面向切面的编程思想和可插拔设计,加强了系统的可维护性和可重用性;拦截器的使用,实现了权限底层拦截的 AOP,提升了系统的安全性;权限标签的设计,既保留了目前工程界使用的权限系统良好的用户体验的优点,又克服了权限系统对业务系统侵入性问题,不需要在界面上统一风格。

2 表单访问权限控制策略

2.1 表单访问权限控制策略机理

传统基于属性的权限控制模型,通过属性实体来实现对数据属性的细粒度权限控制,但在工程中用户一般不能直接访问数据属性,而是通过用户界面中的表单来访问数据属性。一个数据属性可以对应多个表单元素。所以在新策略中增加了对用户接口层的权限控制。新策略对基于属性的权限控制进行了扩展,属性不再是模型控制的原子对象,一个属性可以对应一个或多个表单域对象,通过表单与属性映射表把表单权限映射到数据属性权限,实现了对表单和数据属性的双向权限控制。新策略元素关系如图 2 所示。

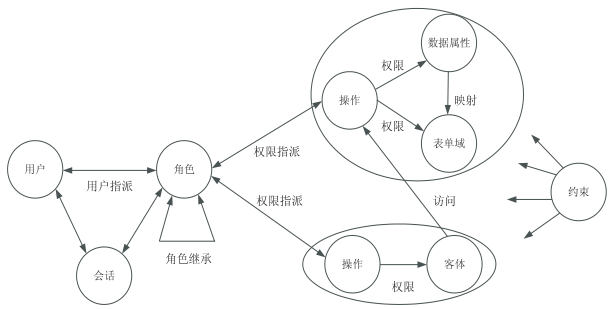

图 2 表单访问控制策略元素关系图

该策略中,在 RABC96 模型的基础上增加了 4 个元素:表单域集合、数据属性集合、表单域许可权集合和数据属性许可权集合。表单域许可权集合是角色到表单域的权限指派,数据属性许可权集合是角色到数据属性的权限指派。数据属性权限是表单域许可权集合映射和数据属性许可权集合的总和。通过客体资源来访问表单域和数据属性权限。

表单域和数据属性权限类型表示为枚举类型{none,readonly,written}:none 表示既没有读权限,又没有写权限,表单域表现为在页面中不显示表单域,数据属性表现为不能执行对该属性数据的查询操作;readonly 为只读权限,只能查看表单域中的数据,不能修改和删除数据,数据属性表现为只能查询该属性数据,不能修改和删除数据;written 为写权限,既可以查

看该表单域中的数据,又可以修改和删除数据,对于数据属性表示拥有对数据属性的查询、修改和删除权限。

2.2　策略形式化描述

上述提出表单访问权限控制机理后,为了对表单访问权限控制进行更一般性的描述,采用康托尔集合论(Cantor's Set)对表单访问权限控制策略进行形式化描述。

定义 1:模型基本元素。

(1)用户对象集 $U=\{u_i \mid i=1,2,\cdots,n\}$;

(2)角色对象集 $R=\{r_i \mid i=1,2,\cdots,m\}$;

(3)数据属性对象集 $A=\{a_i \mid i=1,2,\cdots,j\}$;

(4)表单域对象集 $F=\{f_i \mid i=1,2,\cdots,k\}$;

(5)客体对象集 $N=\{n_i \mid i=1,2,\cdots,l\}$ 。

定义 2:权限指派。

(1)角色之间的继承关系表示为: $\mathrm{RH}=R\times R$;

(2)用户 u 指派角色 r 可以使用二元组 (u,r) 表示,这种指派关系表示为: $\mathrm{UR}=U\times R$;

(3)角色 r 指派表单域资源 f 表示为: $\mathrm{RF}=R\times F$;

(4)角色 r 指派数据属性资源 a 表示为: $\mathrm{RA}=R\times A$;

(5)角色 r 指派客体资源 n 表示为: $\mathrm{RN}=R\times N$;

(6)表单域到属性的映射关系表示为: $\mathrm{fa}:F\rightarrow A$,如果表单域没有属性与之对应,则 $f_i\rightarrow\mathrm{null}$,且表单域到属性是一个非单射。

由模型访问机理知,表单域权限对象集表示为 $p=\{\mathrm{none},\mathrm{readonly},\mathrm{written}\}$ 。

由上述分析知,表单域权限可以使用三元组 (f,a,p) 来表示,其中 f 为表单域资源对象集,fp 为表单域权限对象集。表单域许可权集合可以表示为 $P_f=\mathrm{RF}\times p$ 。数据属性权限是表单域许可权集合映射与数据属性许可权集合的并集,数据属性许可权集合可以表示为 $P_d=\mathrm{RA}\times p$,所以数据属性权限为 $P_a=\mathrm{fa}(P_f)\cup P_d$ 。

2.3　策略安全分析

访问控制模型作为保障系统安全的重要组件,模型的自身安全越来越受到关注。而且目前广泛应用的分散授权对模型的安全性提出了更高的要求,权限泄露[14]成为分散授权中破坏控制系统安全的重要因素。安全分析主要用来分析当前访问控制系统中是否存在权限泄露[14]。文中在角色约束条件下使用图灵机对表单访问控制策略进行安全分析。

定义 3:角色约束。若角色 r 拥有的权限集合不能被更改,则称该角色为成员确定的角色,记为 r^D ;若角色 r 拥有的权限集合可被更改,则称该角色为成员不确定的角色,记为 r^U 。且 $r=r^D\cup r^U$, $r^D\cap r^U=\varnothing$ [15]。

定义 4:角色替代。r' 是 r^U 的关联角色,即 r' 中的权限只能部分决定 r^U 拥有的权限。与角色 r^U 关联的所有集合为 $r_1',r_2',\cdots,r_n'$,令 $R'=r_1'\cup r_2'\cup\cdots\cup r_n'$,那么 r^U 拥有的权限集合可以用 R' 和 r^U 当前拥有的权限集合来表示。

图灵机(TM)分析过程如下[15]:

(1)把角色以字符串的形式表示;

(2)从左到右依次扫描字符,把形如 r^U 的字符用与 r^U 相关的集合 R' 中的所有字符串替代;

(3)如果在第(2)步之后,字符串中只剩下形如 r^U 的字符串,则认为不存在权限泄露;

(4)如果在第(2)步之后,没有进行任何字符置换,且字符串中仍然存在 r^D 相关字符,则认为存在权限泄露;

(5)返回字符串头部,并转到步骤(2)。

当前安全状态是 S ,若非信任安全管理员通过操作 K 状态转化为 S' ,通过图灵机对状态 S' 进行安全分析,若分析结果为存在权限泄露,则认为当前操作是一个非法操作,拒绝当前操作;若分析结果为不存在权限泄露,则认为当前是一个合法操作,允许当前操作。

3　表单访问控制策略设计实现

为降低权限系统与业务系统之间的耦合程度,对表单的权限控制实现基于 Java 标签和 Ajax 技术。页面加载结束后,JavaScript 遍历页面中所有表单中每一个表单域元素,根据表单 ID、表单域元素的 ID 以及认证用户的身份,Ajax 发送异步请求去查询当前用户表单域对象的权限,根据 Ajax 的返回结果,使用 JavaScript 技术动态修改表单中的表单域状态。

上述设计不需要改变表单域元素的风格,克服了中间件提供商必须在界面上统一风格造成对业务系统侵入性问题。

表单访问控制时序图见图 3。

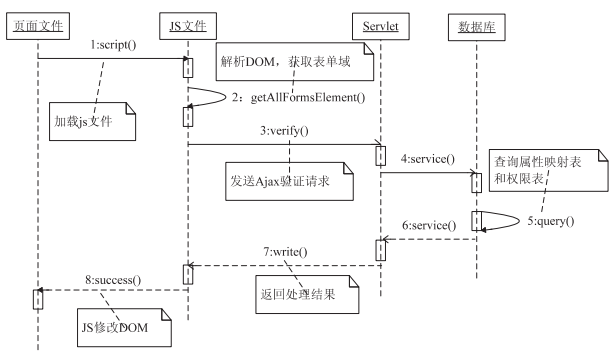

图 3　用户接口访问权限控制时序图

页面文件中 script 标签引入外部权限验证 JS 脚本文件,脚本文件解析 DOM,获取页面中所有表单中的表单域对象,每一个表单域调用 verify( ) 方法发送

Ajax 权限验证请求,Servlet 的 service( )方法接受来自 Ajax 的请求,根据表单对象的 name 属性、表单域元素的 name 属性以及当前用户名称三个参数,验证当前用户对表单域元素的表单域权限,Ajax 接受 Servlet 的返回结果,脚本文件 JavaScript 对 DOM 中的表单域元素进行动态修改。

数据属性的访问控制采用 J2EE 中可插拔的拦截器实现。当客体资源需要访问数据资源时,拦截器会检查当前用户是否拥有对该数据属性的权限。例如当前用户拥有对该数据属性的 readonly 权限,如果用户执行 select 操作,能够正常执行;如果用户执行 update 或 delete 操作,则抛出异常,阻止该操作继续执行。

4 表单访问权限控制模型应用实例

J2EE 是一个企业级开发平台,可以方便地使用 J2EE 平台来实现权限控制。符合 J2EE 规范的组件具有可移植性强、可重用性好、易于维护和可伸缩性好等特点。依托 J2EE 平台实现了表单访问权限控制策略的部分功能。最后,把表单访问控制策略用于学生管理系统的权限控制,用户可以在角色列表界面对角色的表单域权限进行设置,表单访问权限控制用户交互界面见图 4。

图 4 角色表单域权限交互界面图

5 结束语

文中从权限系统的控制粒度和用户交互性角度,提出了一种基于表单访问权限控制策略,并用图灵机对策略进行了安全分析。基于该策略实现的权限系统在保证良好交互性和用户体验的基础上,克服了中间件提供商权限系统在界面上统一风格的限制,降低了权限系统对业务系统的侵入性。但在权限实现过程中,每个权限标签都需要向后台发送Ajax请求,需要频繁与数据库交互,影响了系统性能。因此在后期设计中需要引入缓存设计,减少系统与数据库交互的频率,从而提高系统性能。

参考文献:

[1] 李凤华,苏 锟,史国振,等. 访问控制模型研究进展及发展趋势[J]. 电子学报,2012,40(4):805-813.

[2] 李昕昕,严张凌,王赛兰. 改进的基于角色的通用权限管理模型及其实现[J]. 计算机技术与发展,2012,22(3):240-244.

[3] Freudenthal E,Pesin T,Port L,et al. dRBAC:distributed role-based access control for dynamic coalition environments[C]//Proceedings of the 22nd international conference on distributed computing systems. [s. l.]:IEEE Computer Society,2002:411-420.

[4] Liu S Y,Huang H J. Role-based access control for distributed cooperation environment[C]//Proceedings of 2009 international conference on computational intelligence and security. Beijing,China:IEEE Computer Society,2009:455-459.

[5] Ray I,Yu L J. Short paper:towards a location-aware role-based access control model[C]//Proceedings of the first international conference on security and privacy for emerging areas in communications networks. Athens,Greece:IEEE Computer Society,2005:234-236.

[6] Ray I,Kumar M,Yu L J. LRBAC:a location-aware role based access control model[C]//Proceedings of the second international conference on information systems security. Kolkata,India:Springer-Verlag,2006:147-161.

[7] 张颖君,冯登国. 基于尺度的时空 RBAC 模型[J]. 计算机研究与发展,2010,47(7):1252-1260.

[8] Bertino E,Catania B,Damiani M,et al. GEO-RBAC:a spatially aware RBAC[C]//Proceedings of the 10th ACM symposium on access control models and technologies. New York:ACM Press,2005:29-37.

[9] 熊 智,王 平,徐江燕,等. 一种基于属性的企业云存储访问控制方案[J]. 计算机应用研究,2013,30(2):513-517.

[10] 赵卫东,毕晓清,卢新明. 基于角色的细粒度访问控制模型的设计与实现[J]. 计算机工程与设计,2013,34(2):475-479.

[11] 李 阳. 基于属性 RBAC 的访问控制模型研究[D]. 济南:山东师范大学,2014.

[12] Johnson R. Pivotal software inc[EB/OL]. (2003-03-24)[2013-01-17]. http://projects. spring. io/spring-security/.

[13] Apache. The Apache software foundation[EB/OL]. (2008-02-18)[2014-04-17]. http://shiro. apache. oro/.

[14] 刘 强,姜云飞,李黎明. RBAC 系统的权限泄漏问题及分析方法[J]. 计算机集成制造系统,2010,16(2):431-438.

[15] 杨秋伟,洪 帆,杨木祥,等. 基于角色访问控制管理模型的安全性分析[J]. 软件学报,2006,17(8):1804-1810.

基于表单访问权限控制策略

作者： 吴承来， 周传华， 周家亿， WU Cheng-lai， ZHOU Chuan-hua， ZHOU Jia-yi

作者单位： 吴承来,周传华,WU Cheng-lai,ZHOU Chuan-hua(安徽工业大学 管理科学与工程学院,安徽 马鞍山,243032)， 周家亿,ZHOU Jia-yi(东南大学 计算机科学与工程学院,江苏 南京 ,211189)

刊名： 计算机技术与发展 ISTIC

英文刊名：

年，卷(期)： 2016(2)