第35卷 第24期 计 算 机 工 程 2009年12月
Vol.35 No.24 Computer Engineering December 2009
·安全技术· 文章编号：1000—3428(2009)24—0165—03 文献标识码：A 中图分类号：TP309.2

扩展 RBAC 模型及其在 ERP 系统中的应用

于小兵，郭顺生，杨明忠
(武汉理工大学机电工程学院湖北省数字制造重点实验室，武汉 430070)

摘 要：基于 Core RBAC 模型，提出扩展 RBAC(基于角色访问控制)模型。该模型细化了客体集、操作集，提出了组别的概念，并对权限进行三维约束，实现了面向应用的 RBAC 体系结构，增强了系统的安全性和易维护性。结合企业信息化的典型代表——ERP 系统，对扩展 RBAC 模型的具体实施进行分析。企业应用结果表明，该模型适用于企业信息化建设。

关键词：基于角色访问控制；客体集；企业资源计划

Extended RBAC Model and Its Application in ERP System

YU Xiao-bing, GUO Shun-sheng, YANG Ming-zhong
(Hubei Digital Manufacturing Key Laboratory, School of Mechanic and Electronic Engineering, Wuhan University of Technology, Wuhan 430070)

【Abstract】 This paper presents an extended Role-Based Access Controls(RBAC) model based on Core RBAC model. The model discusses object sets and operation sets in detail, established groups. It carries out restrictions on power in three dimensions and realized application-oriented architecture. It enhances security and maintenance. The model is applied to Enterprise Resourse Planning(ERP) system. It is the typical representative of enterprise information system. Application result in enterprise shows that the extended model is totally suitable to it.

【Key words】 Role-Based Access Controls(RBAC); object sets; Enterprise Resourse Planning(ERP)

1 概述

随着企业信息化建设的不断深入，日益积累的信息资源对企业生存、发展起着重要的作用。因此，如何有效地保护这些资源就成为一个重要的研究课题。目前，国内外对资源的访问控制研究主要集中在任意访问控制(DAC)、强制访问控制(MAC)[1-2]和基于角色的访问控制(RBAC)[3]。

由于应用复杂度的不断提高，DAC 和 MAC 越来越显现出局限性，几乎静态化的个体资源控制已经无法适应复杂多变的应用系统——资源的变动、人员的变动。在这种情况下，RBAC 被广泛的应用。然而，由于 RBAC 概括了任何系统的访问控制，没有足够的细化[4]，没有对企业信息化这一特殊的信息系统进行阐述。本文在 RBAC 模型的基础上，提出了扩展 RBAC 模型，并应用于汽车改装企业 ERP 系统的访问控制中，取得了良好的效果。

2 Core RBAC 模型

图 1 为 Core RBAC 模型[5]。其中，USERS, ROLES, SESSIONS, PRMS, OPS 和 OBS 分别代表用户集、角色集、会话集、权限集、操作集和客体集。

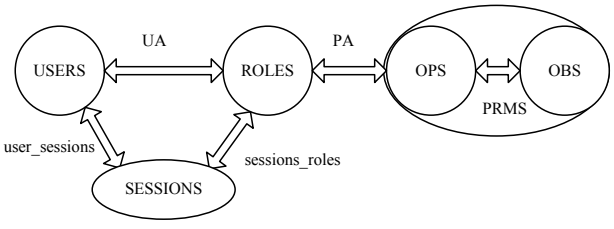

图 1 Core RBAC 模型

它们之间的关系如下：

(1)UA⊆USERS × ROLES，建立 USERS 和 ROLES 之间多对多的映射关系，使 USERS 隶属于某个或者某些角色。

(2)assigned_users:(r:ROLES) → 2^{USERS}，ROLES 和它对应 USERS 之间的映射关系：

assigned_users(r)={u∈USERS|(u, r)∈UA}

(3)PRMS=$2^{(OPS\times OBS)}$，建立权限集，由 OPS 和 OBS 构成。

(4)PA⊆PRMS×ROLES，建立 PRMS 和 ROLES 之间多对多的映射关系。

(5)assigned_permissions(r:ROLES)→2^{PRMS}，ROLES 和它对应 PRMS 之间的映射关系：

assigned_permissions(r)={p∈PRMS|(p, r)∈PA}

(6)Op(p:PRMS)→{op⊆OPS}，建立 op 和 OPS 之间的隶属关系。

(7)Ob(p:PRMS)→{ob⊆OBS}，建立 ob 和 OBS 之间的隶属关系。

(8)user_sessions(u:USERS)→$2^{SESSIONS}$，建立用户 u 和 SESSIONS 之间的映射关系。

(9)session_roles(s:SESSIONS)→2^{ROLES}，建立 s 和 ROLES 之间的映射关系：

session_roles(si)⊆{r∈ROLES|(session_users(si), r)∈UA}

(10)avail_session_prms(s:SESSIONS)→2^{PRMS}，建立 SESSIONS 和 PRMS 之间的映射关系。

基金项目：国家科技部国际合作基金资助项目“基于多智能体的数字制造基本理论与关键技术研究”(2006DFA73180)；湖北省科技攻关计划基金资助项目“机械制造业(含汽车)ERP/SCM/CRM 集成技术与系统攻关”(2006AA108A03)

作者简介：于小兵(1983－)，男，博士研究生，主研方向：ERP 系统，电子商务；郭顺生、杨明忠，教授、博士生导师

收稿日期：2009-05-10 **E-mail：**yuxb111@163.com

从图 1 可以看出 RBAC 的优点：在用户和权限间加入了角色层。通过将权限赋予角色，再将角色分配至用户。由于角色变动没有用户频繁，这样可以减少分配权限的负担。它具有易于使用的特点。然而，由于 RBAC 概括了任何系统的访问控制，对用户、角色、会话、权限等没有足够的细化，无法满足企业信息化建设的特殊需求，如 ERP 系统的建设。因此需要对 Core RBAC 做进一步的扩展，以满足特殊系统的需求。

3 扩展 RBAC 模型

本文在 Core RBAC 模型基础上，提出了适合企业信息化系统的访问控制模型扩展 RBAC，如图 2 所示。

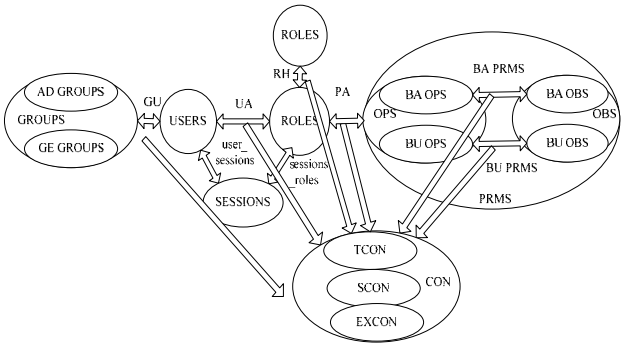

图 2 扩展 RBAC 模型

该模型沿用了 Core RBAC 模型中的各个基本概念，并扩展了 GROUPS，细化了 OPS 和 OBS，建立了约束机制 CON。在图 2 中，GROUPS, AD GROUPS, GE GROUPS, RH, BA OBS OPS, BA OBS, BA PRMS, BU OBS OPS, BU OBS, BU PRMS, CON, TCON, SCON 和 EXCON 分别表示组、管理员组、一般组、角色继承、基础客体集操作、基础客体集、基础客体操作权限集、业务客体集操作、业务客体集、业务客体操作权限集、约束、时间约束、空间约束、排它约束。与 Core RBAC 中的 ROLES 面向软件不同，这里的 GROUPS 是面向应用的。企业内部的各个部门就类似 GROUPS。GE GROUPS 是一般的组，不会具有系统的所有权限；AD GROUPS 则具有系统所有的权限。对企业信息化系统，AD GROUPS 一般隶属信息化办公室或者信息化维护小组所有。基础客体集(BA OBS)一般是在信息化软件初始化的时候，进行参数的设置。这些信息在系统运行以后一般不会做调整，如中国省、市名称及其隶属关系。而业务客体集(BU OBS)是系统运行之后，建立的一些资源文件或者数据，如销售订单、采购订单等信息。基础客体集支撑着业务客体集的运行。

(1)GROUPS, AD GROUPS 和 GE GROUPS 三者关系如下：

GROUPS＝AD GROUPS∪GE GROUPS

AD GROUPS∩GE GROUPS＝Ø

(2)GU⊆GROUPS×USERS，建立 GROUPS 和 USERS 之间多对多的映射关系。对于管理规范的企业，员工一般只隶属一个部门，USERS 和 GROUPS 之间是一对多的关系。由于多对多的范围更大，因此本文把一对多的问题也考虑在内。

(3)assigned_groups:(u:USERS)→2^{GROUPS}，USERS 和它对应 GROUPS 之间的映射关系如下：

assigned_groups (u)={g∈GROUPS|(g, u)∈GU}

(4)OBS, BA OBS 和 BU OBS 三者关系如下：

OBS＝BA OBS∪BU OBS

BA OBS∩BU OBS＝Ø

(5)BA PRMS=$2^{(BA\ OPS\ \times BA\ OBS)}$，建立基础客体操作权限集，由 BA OPS 和 BA OBS 构成。

(6)Op(p:BA PRMS)→{op⊆BA OPS}，建立 op 和 BA OPS 之间的隶属关系。

(7)BU PRMS=$2^{(BU\ OPS\times BU\ OBS)}$，建立业务客体操作权限集，由 BU OPS 和 BU OBS 构成。

(8)Op(p:BU PRMS)→{op⊆BU OPS}，建立 op 和 BU OPS 之间的隶属关系。

(9)OPS, BA OPS 和 BU OPS 三者关系如下：

OPS＝BA OPS∪BU OPS

BA OPS∩BU OPS＝Ø

(10)PRMS, BA PRMS 和 BU PRMS 三者关系如下：

PRMS＝BA PRMS∪BU PRMS

BA PRMS∩BU PRMS＝Ø

(11)约束集 CON ={TCON,SCON,EXCON}，它是三元组，用于约束角色间的继承、用户的多角色、操作集对客体集，避免权限相互矛盾或者越权情况的发生。其中，TCON 和 SCON 的约束主要是获得该角色的时间段、网络段和区域段的约束条件；EXCON 指一个用户只能同时获得互斥角色中的一个。

4 扩展 RBAC 模型案例分析

本文将扩展 RBAC 模型应用到汽车改装企业 ERP 系统的权限访问控制中。该系统的主要功能是实现对汽车改装企业全面的信息化管理，具体包括：订单管理，采购管理，采购质检管理，材料入库管理，材料出库管理，装罐车间管理，热处理车间管理，涂料车间管理，检测车间管理，库存管理，成本管理等。用户通过该系统，可以完成信息的录入、检索、编辑、删除、打印、产生报表等各种操作。系统涉及改装企业的各个部门。如果单纯采用 Core RBAC 模型，管理起来就比较混乱。本文采用扩展 RBAC 模型，建立用户组别、基础客体集、业务客体集、操作权限集，对系统的访问权限实施动态管理。

4.1 扩展 RBAC 的初始化

根据系统的功能，对扩展 RBAC 中可能涉及到的内容进行初始化，具体如下：

AD GROUPS={信息化小组}

GE GROUPS={销售部，采购部，技术中心，准备车间，装罐车间，热处理车间，涂料车间，检测车间，仓库，经理办，财务}

BA OBS={部门信息，人员信息，地区信息，物料信息，库区信息，产品信息，材料信息，报表格式信息}

BU OBS={产品订单信息，成品计划信息，材料采购信息，材料质检信息，质检退货信息，材料入库信息，材料出库信息，仓库发料信息，材料退库信息，产品质检信息，产品入库信息，产品出库信息，售后服务信息，成本核算信息}

OPS={增加，修改，删除，审核，撤销审核，打印，生成 excel 报表，生成 word 报表}

BA OPS=BA OBS × OPS

BU OPS= BU OBS × OPS

4.2 扩展 RBAC 的授权过程

图 3 为扩展 RBAC 在汽车改装企业 ERP 系统中的具体应用过程。其中，(1)AD GROUPS 登录身份认证服务器；(2)校验 AD GROUPS 输入的登录信息；(3)AD GROUPS 登录成功，进入 Extended RBAC 授权管理服务器；(4)通过授权管理界

面，对 GE GROUPS 用户进行授权；(5)GE GROUPS 登录身份认证服务器；(6)校验 GE GROUPS 输入的登录信息；(7)GE GROUPS 登录成功，进入汽车改装企业 ERP 业务管理服务器；(8)、(9)通过 ERP 界面，GE GROUPS 进行相关业务管理操作

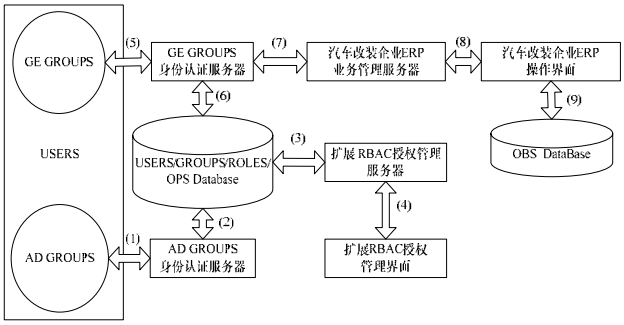

图 3　ERP 实施中的扩展 RBAC 授权过程

该过程中的主要构成部分如下：

(1)AD GROUPS 身份认证服务器：对 AD GROUPS(信息化小组)的身份和角色进行验证。这里没有将 AD GROUPS 和 GE GROUPS 身份认证服务器放在一起，主要是为了解耦。

(2)扩展 RBAC 管理界面：通过图形化界面定义 USERS/GROUPS/ROLES/OPS，实现用户到角色的分配、用户到组别的分配、角色对客体操作权限的分配。通过 Extended RBAC 授权管理服务器，将这些信息存储到 USERS/GROUPS/ROLES/OPS 数据库中。

(3)扩展 RBAC 授权管理服务器：主要负责对 USERS/GROUPS/ROLES/OPS 数据库进行管理，例如增加、修改、删除等操作，与 Extended RBAC 管理界面一起组成扩展 RBAC 管理系统，如图 4 所示。

(4)USERS/GROUPS/ROLES/OPS 数据库：存放 AD GROUPS 通过扩展 RBAC 管理系统定义的组别、角色集、操作集、权限集、每个用户所属的组别、每个用户所属的角色。

(5)GE GROUPS 身份认证服务器：对 GE GROUPS 的身份和角色进行验证。

(6)OBS 数据库：存放各种基础数据和业务逻辑数据。

图 4　扩展 RBAC 授权管理界面

5　结束语

本文对 Core RBAC 模型进行了扩展，提出了适合企业信息化系统的扩展 RBAC 模型。结合汽车改装企业 ERP 实施的具体情况，将扩展 RBAC 模型应用其中。实践表明：扩展 RBAC 模型不仅没有和 ERP 系统有任何的耦合，简化了企业信息化建设过程中的访问控制；另一方面，它细化了客体集、操作集，提出了组的概念，提升了系统的安全性、易维护性。

参考文献

[1] 金琼琤, 杨树堂, 蒋兴浩, 等. 基于 T-RBAC 的企业权限管理方法[J]. 计算机工程, 2004, 30(19): 93-95.

[2] 曹勇刚, 金茂忠, 刘　超. CMS 中 RBAC 模型的改装和应用[J]. 北京航空航天大学学报, 2005, 31(10): 1153-1158.

[3] David F, Richard K. Role-based Access Controls[C]//Proceedings of NIST-NCSC'92. Baltimore, Maryland, USA: [s. n.], 1992: 554-563.

[4] 梁　彬, 孙玉芳, 石文昌, 等. 一种改进的以基于角色的访问控制实施 BLP 模型及其变种的方法[J]. 计算机学报, 2004, 27(5): 636-644.

[5] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

编辑　金胡考

(上接第 164 页)

效解密算法，与采用直接解密算法相比，大大减少了逻辑单元的占用。加密/解密模块部分在 1 个时钟周期内完成轮变换的 1 个运算，与在 1 个时钟周期内完成 1 次轮变换相比，提高了处理速度。对于 32 位、64 位等数据路径的 AES IP 核，可以通过修改密钥加载模块、明文/密文加载模块和密文/明文模块实现。

参考文献

[1] AES IP Core Introduction[EB/OL]. (2008-04-08). http://www.dilloneng.com/fft_ip/other_ip/aes.

[2] AES Cores[EB/OL]. (2007-08-09). http://www.heliontech.com/aes.htm.

[3] Hardware IP Cores of Advanced Encryption Standard AES_Rijndael[EB/OL]. (2008-04-12). http://bass.gmuedu/crypto/ rijndael.htm.

[4] 曾　毅, 鲁　欣, 付宇卓. 一种优化可配置的 AES 密码算法硬件实现[J]. 微电子与计算机, 2004, 21(12): 34-37.

[5] National Institute of Standards and Technology. Federal Information Processing Standards(FIPS) 197 Advanced Encryption Standard[S]. 2001.

编辑　张正兴