B/S环境下CIMS安全模型设计与实现

刘孝保[1]，杜平安[1,2]

(1. 电子科技大学机械电子工程学院 成都 610054; 2. 机械制造系统工程国家重点实验室 西安 710049)

【摘要】随着网络被非法攻击的可能性增大，提出了一种B/S环境下的基于角色的访问控制双层模型。该模型将RBAC合理运用于数据库层和Web容器层。同时辅以基于角色的菜单定制形成系统安全模型，将角色融入到系统的各个应用层面，统一管理系统各个应用层面的系统资源，从多个层面来保护系统安全。利用这种安全模型，采用Oracle9i/BES6.5/j2ee技术设计，实现了一套浏览器/服务器环境下的计算机集成制造系统的安全管理子系统。

关 键 词 浏览器/服务器环境; 计算机集成制造系统; 基于角色的访问控制; 安全模型

中图分类号 TP309.2 **文献标识码** A

Design and Implementation of Role-Based CIMS Security Model under B/S Environment

LIU Xiao-bao[1]，DU Ping-an[1,2]

(1. School of Mechatronics Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. State Key Laboratory for Manufacturing Systems Engineering Xi'an 710049)

Abstract Role-based access control (RBAC) is a major technology in computer integrated manufacturing systems (CIMS)'s security management. In this paper, a double-layer RBAC model under B/S environment is presented. In this model, RBAC is applied to both database layer and web container layer. Furthermore，A CIMS security model is established with the help of role-based custom-built menu technology. This security model is applied to all application layers to protect the system resource located at different application layers. Using this security model and the technology of Oracle9i/BES6.5/j2ee, a CIMS's security management system under B/S environment is realized.

Key words B/S environment; computer integrated manufacturing systems(CIMS); role-based access control; security model

随着互联网技术的迅猛发展，CIMS开始从传统的C/S模式向B/S模式转变。由于HTTP和浏览器本身的原因使得系统被非法攻击的可能性增大，这就给系统的安全性提出了更高的要求。针对B/S的结构特点，除了使用传统的“户名/密码”安全验证方式以外，还需采用其他安全保护措施。

由于安全性、方便性和灵活性等特点，基于角色的访问控制(role based access control，RBAC)已成为CIMS的主要安全技术。目前，多数数据库管理系统(database management system，DBMS)和Web容器都支持RBAC。但在B/S模型下，由于角色管理的系统资源位于不同的应用层面，使得RBAC并没能完全融入应用系统中。为此，本文提出一种RBAC双层模型，同时辅以基于角色的菜单定制，构成系统完整的安全模型。

1 系统安全方案模型

系统安全模型结构如图1所示。

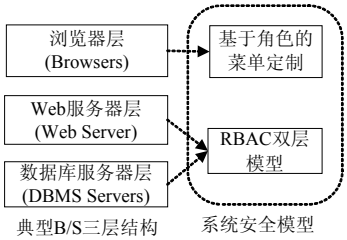

图1 系统安全模型体系结构图

RBAC是文献[1]提出的一种安全访问控制模型，用以解决具有大量用户、数据客体以及访问权限的系统安全管理问题[2]。其核心思想是利用“角色”这一“中介”将用户和权限分离以简化权限管理[2]。目前，多数DBMS和Web容器都支持RBAC，

收稿日期：2006－03－28；修改日期：2006－07－13
基金项目：国家863/CIMS主题资助项目(2003AA411210)
作者简介：刘孝保(1978－)，男，博士生，主要从事ERP/CAE方面的研究.

但由于B/S模式下二者处于不同应用层面，因此不能直接将二者的RBAC合理地利用到系统中来。

针对B/S的Browsers/Web Server/DBMS Servers经典结构，并结合RABC的核心思想，本文从保护系统各个应用层面资源出发，从应用的角度提出了一个新的RBAC双层模型，如图2所示。该模型采用集中管理的权限维护方式，可以充分利用数据库和Web容器本身支持的RBAC，将RBAC合理运用于数据库层和Web容器层。该模型将应用于B/S结构下的数据库层和web容器层。

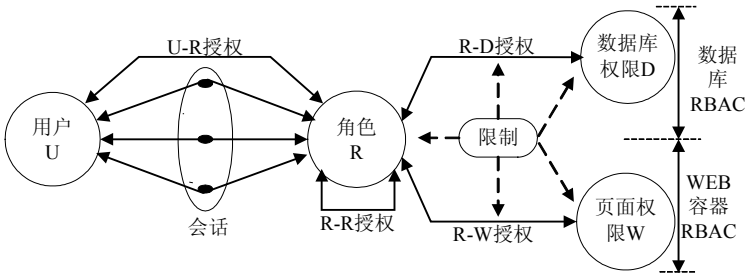

图2 RBAC双层模型示意图

定义 用户集合：$U=\{u_1,u_2,\cdots,u_i\}$；角色集合：$R=\{r_1,r_2,\cdots,r_j\}$；数据库权限集合：$D=\{d_1,d_2,\cdots,d_m\}$；页面权限：$W=\{w_1,w_2,\cdots,w_n\}$；系统权限集合：$P=W+D$。U、R、P之间为多对多的关系，即一个用户可授权多种角色，同一角色可授权给多个用户；同一个角色可对多个资源有访问权限，同一资源也可授权给多个角色[3]。基于如上模型及定义，可得出以下结论：

结论1 系统共享用户、角色及其授权关系信息，但由于系统资源位于不同的应用层面，需根据不同层面权限特点来合理安排访问权限验证方式。

结论2 角色作用在两个不同的应用层面，数据库层和Web容器层。该模型是这两个层面RBAC的有机结合。对于任何一个应用层面来说，都需按照其层面特点来组织管理本层面的RBAC。

结论3 将权限P授权给角色r_j用$A(r_j, P)$表示；角色r_j继承角色r_k用$I(r_j, r_k)$表示，则用户最终的权限集合为：

$$P=\bigcup_{j=1}^{n}(A(r_j,P)+A(I(r_j,r_k),P))=$$
$$\bigcup_{j=1}^{n}\begin{pmatrix}A(r_j,W)+A(r_j,D)+\\A(I(r_j,r_k),W)+A(I(r_j,r_k),D)\end{pmatrix}$$

用户的权限集合为他所授权角色的页面资源权限、数据库资源权限、以及所继承角色的页面资源权限、数据库资源权限的总和。对上述模型的实际运用，应该注意：(1) 需根据系统实际运行环境对系统角色进行合理划分，使角色具有一定的实际意义的同时也能够满足权限最小原则[4]。(2) 由于上述的RBAC是运行在两个不同的应用层面上，因此需要使用一种合适的同步映射机制将两个层面的角色进行关联，将二者的RBAC有机结合。(3) 角色可以继承，但不能循环继承，同时应该尽量减少继承级数。角色以偏序关系(记为“≥”)组织，如果$x\geqslant y$，那么角色x就继承了角色y的权限[4]。当$R_a\geqslant R_b$、$R_b\geqslant R_c$、$R_c\geqslant R_a$，将会造成权限继承的“死循环”，所以不能循环授权。同时，系统在处理偏序问题时一般采用递归算法，因此偏序级数将是影响系统运行开销的一个重要指标，应该尽量减少偏序级数。

2 系统安全设计与实现

针对B/S应用系统的访问流程特点，系统安全访问控制流程设计如图3所示。针对图3系统安全访问流程设计，结合RBAC双层模型，系统安全管理设计思路为：系统管理员通过前台(浏览器)进行系统安全管理，将管理相关数据保存在数据库数据表中，利用数据库触发器将安全管理同步反映到DBMS以利用数据库本身的RBAC安全策略，完成对数据库安全管理；对页面资源管理则通过Web.xml配置文件的安全角色配置以利用Web容器自身支持的RBAC；最后根据合法登陆用户的授权角色形成动态操作菜单。以Oracle数据库和BES(borland enterprise server)网络服务器来设计系统安全[6]。

2.1 数据库设计

数据库设计是系统安全设计的基础和核心。对于图3中的RBAC应用模型，数据库功能为：保存应用系统安全的相关数据；将保存在数据表中的授权主体(如用户、角色)以及授权关系同步反映到数据库管理系统。基于以上目的，数据库设计分为两个方面：数据表和触发器设计。

2.1.1 数据表设计

数据表用于保存安全模型实现的相关数据，包括授权主体信息、授权信息。由于oracle对中文支持

较好，为了系统维护和开发的方便，采用中文来定义数据库对象。用Power Designer表示的数据库物理模型设计如图4所示。图中“角色信息”、“用户信息”保存授权主体的信息；“用户权限信息”、“权限委托信息”保存授权信息。由于数据库授权客体已经记录在DBMS的数据字典中且不需要对其进行附加信息记录，因此不必设计相关的数据表，在授权的时候查询数据库数据字典即可。

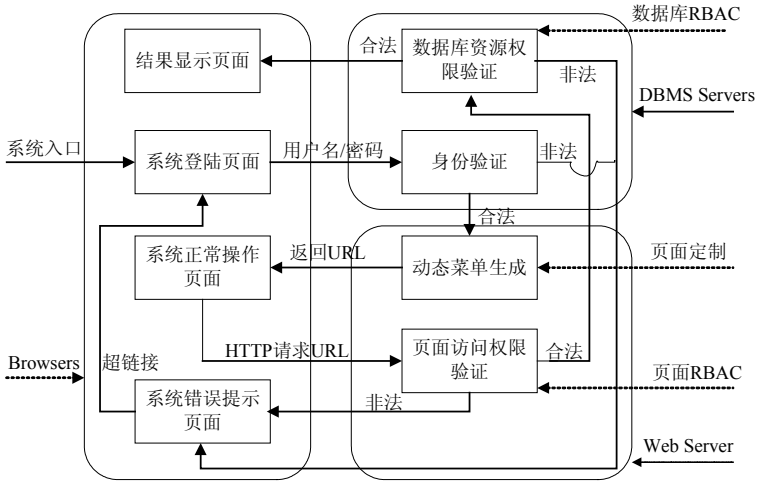

图3　系统访问控制流程图

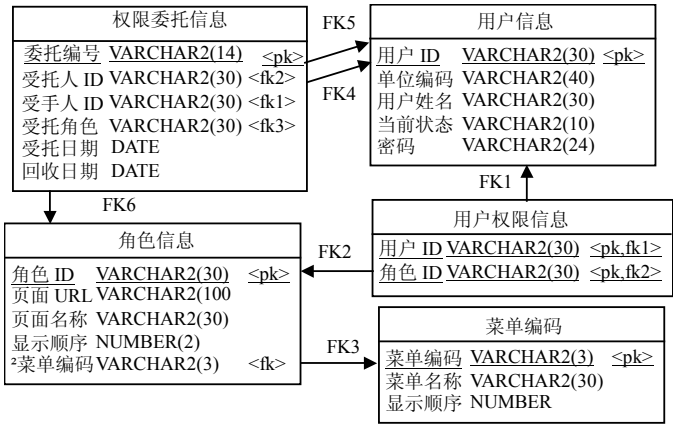

图4　数据库物理模型设计

2.1.2　触发器设计

根据图2所示的模型，为了利用数据库自身的RBAC，需建立RBAC在数据库中的映像——数据库角色与用户及其授权关系。由于触发器可以简化程序开发以及减少系统开支和方便系统维护，因此采用触发器来完成。分别为图4中的“角色信息”“用户信息户”“权限信息”和“权限委托信息”建立相应的Delete、Insert、Update触发器，将用户对数据库表进行的操作同步反映到数据库管理系统中。以“角色信息”表为例，为其创建一个Insert触发器。当增加一条记录(即创建一个角色)时，触发器执行一条为DBMS创建角色的DDL，在数据库中创建该用户，这样就可以利用数据库本身的RBAC了。

由于触发器的同步操作，一个系统用户对应于一个数据库用户，因此系统的用户身份验证和访问验证权限验证就可以利用数据库本身的验证机制来实现，以减少编程工作量和提高验证效率。

2.2　RBAC授权管理设计

RBAC授权管理设计是基于数据库设计并体现RBAC的。针对B/S的结构特点，RBAC的授权管理就相应地涉及到数据库管理系统和Web容器两个应用层面的授权管理[7]。RBAC授权管理框图如图5所示。由于系统授权客体(这里是指数据库资源、网页资源)相对固定，所以不涉及授权客体维护内容。为了管理的方便，RBAC授权管理采用前台管理的方式进行，并通过触发器和应用程序将前台管理结果同步反映到数据库层和Web容器层[7]。管理员必须合法登陆系统安全管理模块后才能进行RBAC授权管理，其授权管理流程如图6所示。

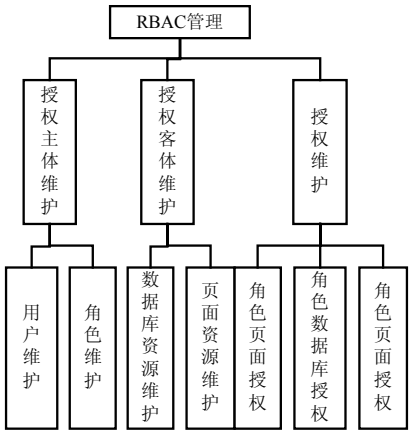

图5 RBAC授权管理框图

2.2.2 授权管理

授权管理的目的是建立授权主体和授权客体之间的联系，包括角色/数据库授权和角色/网页授权以及用户/角色授权。角色/数据库授权将授权信息保存到数据表的同时也需利用触发器将授权信息同步到DBMS中，以利用DBMS所支持的RBAC。角色/网页授权将安全角色的授权信息以XML格式保存到Web容器配置文件Web.xml中，以利用Web容器的RBAC。用户/角色授权是将角色授权给用户，使该用户拥有其授权角色的相应访问权限。当合法用户访问系统资源时，系统根据用户角色来判断所访问的数据库资源以及网页资源是否已授权，如果授权则访问成功，否则将返回“权限不足”的错误信息。

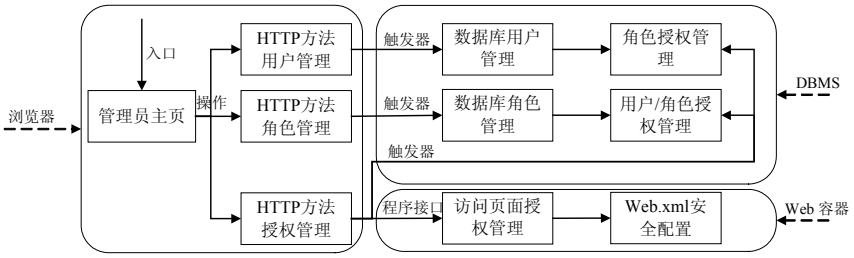

图6 RBAC授权管理流程

2.3 菜单定制设计

当登录用户合法性验证通过后，系统需对用户的操作菜单进行用户定制：根据该用户所授权角色访问资源进行限制，防止用户非法操作没有授权的页面，同时也使得界面更加美观、简洁。其实现方式为：从数据库“用户权限信息表”和“权限委托信息表”中检索出该用户角色的合法操作页面URL，并根据用户需求进行操作菜单分组，生成为用户定制的页面操作菜单。

3 应用实例

本文利用安全模型以及Oracle9i/BES6.5/ J2EE技术开发了一套B/S结构的CIMS，该系统的安全管理以角色为中心，通过角色创建并给角色授予数据库权限和页面权限，然后将该角色授权给用户，从而使该用户拥有相应的系统资源访问权限。由于双层RBAC模型的实现分别通过Oracle数据库本身RBAC策略和Web容器的发布描述文件的配置，因此系统业务模块的编程将不涉及安全模块。这样，安全管理与其他业务模块相互分离，使编程工作量减少而开发效率和系统安全管理的灵活性得到提高。目前，该系统已用于一家租赁企业并运行良好。

4 结束语

针对B/S环境的特性，利用RBAC双层模型，从保护系统资源和充分利用数据库和Web容器本身的RBAC角度出发来构建系统的安全策略，从系统的各个应用层面来实现系统资源的保护。另外，现实生活中很多不安全因素并不是技术原因造成的，而是由于管理不规范所造成的。因此，除了在技术方面应用先进的安全管理策略以外，更要规范、完善系统的人文管理，给系统安全、有序的运行环境。

参 考 文 献

[1] PARK J S, SANDHU R, AHN G. Role-based access control on the web[J]. ACM Transactionson Information and System Security, 2000, 4(1): 37-71.
[2] 张东站, 薛劲松, 宋瀚涛. 基于I-RBAC的CIMS集成访问控制[J]. 计算机集成制造系统, 2004, 10(1): 50-54.
[3] 严 悍, 张 宏, 许满武. 基于角色访问控制对象建模及实现[J]. 计算机学报, 2000, 23(10): 1064-1071.
[4] 桂艳峰, 林作铨. 一个基于角色的Web 安全访问控制系统[J]. 计算机研究与发展, 2003, 40(8): 1186-1194.
[5] 高正宪, 李中学. Web环境下基于角色的访问控制策略及实现[J]. 计算机工程, 2004, 30(8): 133-135.
[6] 刘孝保, 杜平安. J2EE模式下基于角色的访问控制的应用研究[J]. 计算机应用, 2006, 23(06): 1331-1333.
[7] 张方舟, 王东安. 采用J2EE安全机制支持RBAC模型的研究和实现[J]. 计算机工程, 2006, 23(13): 125-127.

编 辑 税 红