基于多粒度权限的访问控制

叶春晓[1,2]，符云清[3]，吴中福[1]，李　云[1]

(1. 重庆大学 计算机学院，重庆 400044；2. 重庆大学 应用技术学院，重庆 400030；3. 重庆大学 网络教育学院，重庆 400044)

摘　要: 基于角色的访问控制在权限管理中得到广泛的应用。在实际系统中，通过对系统权限的多粒度划分，实现对系统权限的有效管理。对相关概念和操作进行了形式化定义，在此基础上描述了权限互斥和角色互斥关系。给出了重要过程的流程图和主要表之间的关系。

关键词: RBAC; 权限控制; 多粒度权限

中图法分类号: TP309.2　　**文献标识码**: A　　**文章编号**: 1001-3695(2004)10-0087-03

Access Control Based on Multi-granularity Privileges

YE Chun-xiao[1,2], FU Yun-qing[3], WU Zhong-fu[1], LI Yun[1]

(1. *School of Computer, Chongqing University, Chongqing* 400044, *China*; 2. *College of Applied Science & Technology, Chongqing University, Chongqing* 400030, *China*; 3. *College of Network Education, Chongqing University, Chongqing* 400044, *China*)

Abstract: RBAC has gained a wide application in privilege management. It has access an efficiency management of system privilege in a real system, by the means of a multi-granularity privileges division. This papers proposes some concepts and these formal definitions, descript mutex relations of privileges and of roles, illustrate some important workflow and relations among some main tables.

Key words: RBAC; Access Control; Multi-granularity Privilege

访问控制作为信息系统的安全技术，获得了极大的发展。而基于角色的访问控制技术——RBAC[1]，作为信息完全领域的一种新技术，正不断受到重视。其中具有代表性的模型为 Sandhu 提出的 RBAC96 模型，该模型一经提出，即受到瞩目，在此基础上人们又提出了许多补充和改进模型[2]。相关的标准也在研究发布中。

在变电站管理系统中，利用 RBAC 思想，将角色引入到访问控制中，实现对系统中用户操作权限的多粒度控制[3]。

1　基本思路

1.1　权限设置

RBAC 中，权限是主体对客体所能执行的操作。在常见的商用数据库中，权限可体现为对表的查询、插入、删除和修改操作等原子操作。但在用户实际使用中，不可能将权限定义为这些基本操作，否则系统管理员在进行权限指派时必须对相关数据库有深入的了解，这将加大系统管理员的工作难度。在本系统中，将权限定义为与用户业务相关的操作，同时对权限进行多粒度划分，以适应用户的实际需要。

可将权限定义为如下几个层次:

(1) 系统功能层

该层所表示的权限范围较大，主要是系统中的子系统或者子模块。子系统和子模块在系统中以系统菜单的形式表现，因而对用户来说，就是他所能够执行的系统功能菜单。系统功能层权限也就控制了用户对相关子系统菜单是否有执行权限。显然，对系统中的不同用户来说，其所能执行的功能是不同的。

定义 1　P_F 为系统功能层权限集合，$p_f[i]$ 为其中第 $i(1 \leq i \leq n, n$ 为系统的子系统或子模块数) 个权限。

本系统的 P_F = {运行记录、设备管理、查询统计、操作票管理、一种工作票管理、二种工作票管理、动火工作票管理、安全质量考核、系统维护}。

(2) 页面层

页面层实际上就是子功能层，即系统主菜单下的子菜单。由于受 Web 方式下的显示限制，页面的菜单层次以二层为宜，用户选择了子菜单就直接进入页面。将本层作为权限的一级主要是控制用户能够进入的页面。将页面层单独出来而不是作为系统功能层的一部分的主要考虑是，可以将某个子系统或子模块作为一个整体赋予用户，同时用户也可以只拥有该子系统或子功能下部分子功能，方便系统管理员的权限指派和管理工作。

定义 2　P_p 为页面层权限集合，P_p^i 为第 i 个系统功能层权限 $p_f[i]$ 下的页面层权限集合。$P_p^i[j]$ $(1 \leq j \leq m, m$ 为第 i 个系统功能层权限下的页面层权限数) 为第 j 个页面层权限。

例如，设 P_p^4 为操作票管理下的页面权限集合，则 P_p^4 = {操作票填写、操作票审批、操作票终止、操作票回收}。

(3) 操作层

对某一具体页面来说，不同用户所能执行的操作不一样。以运行记录页面为例，该页面包含四个按钮(即四种不同的操作): 添加、删除、修改、打印。不同的操作代表了对该页面数据的不同权限。所有用户均具有只读查询权限，值班用户具有

收稿日期: 2003-08-10; 修返日期: 2003-11-13

添加和打印权限,值班长除了添加和打印权限外,还具有删除和修改权限。这样,将权限细分到操作层后,就可以达到更细粒度的权限控制。

定义3 P_o 为操作层权限集合,P_o^i 为第 i 个页面层权限 P_p^i 下的操作层权限集合。$P_o^i[k]$ ($1 \le k \le t$, t 为第 i 个页面层权限下的操作层权限数) 为第 k 个页面层权限。

例如,设 P_o^1 为操作票填写下的操作权限集合,则 P_o^1 = {添加,修改,打印}。

1.2 角色设置

RBAC 中,为方便对权限的管理,引入了角色概念。角色就是权限的集合。有了角色后,将用户赋予相应的角色即是将权限赋予相应的用户。角色的设置主要考虑到两个因素: 一个是现实中实际用户的职责,即用户所从事的工作; 二是用户单位的组织结构,即用户所处的职务。

定义 4 ROLE 表示系统的角色集合, role[i] ($1 \le i \le m$, m 为系统角色总数) 表示其中的第 i 个角色。

在本系统中,设置了以下主要角色:

系统管理员(sa) ,数据维护员(dm) ,操作员(op) ,班长(monitor) ,签字人员(sig) ,安全人员(sec) ,副局长(ddg) ,局长(dg) 。

在本系统中,有 ROLE = { sa, dm, op, monitor, sig, sec, ddg, dg} 。

1.3 用户设置

系统用户即为使用本系统的各个人员。

定义 5 USER 表示系统的用户集合, user[i] ($1 \le i \le n$, n 为系统用户总数) 表示其中的第 i 个用户。

1.4 角色 - 权限指派

首先考虑权限之间的互斥[4]情况。

定义 6 分下述三种情况:

情况 1 对于权限 $p_f[i]$, $p_f[j]$, 若$\forall$ role[k] $\in$ ROLE, 使得 $p_f[i]$, $p_f[j]$ 不能同时赋予 role[k] ,则称 $p_f[i]$, $p_f[j]$ 是互斥系统功能层权限,记为 $p_f[i] \perp p_f[j]$;

情况 2 对于权限 $P_p^i[i]$, $P_p^i[j]$, 若$\forall$ role[k] $\in$ ROLE, 使得 $P_{p[i]}^i$, $P_{p[j]}^i$ 不能同时赋予 role[k] ,则称 $P_{p[i]}^i$, $P_{p[j]}^i$ 是第 i 个系统功能层下的互斥页面层权限,记为 $P_{p[i]}^i \perp P_{p[j]}^i$;

情况 3 对于权限 $P_{o[i]}^i$, $P_{o[j]}^i$, 若$\forall$ role[k] $\in$ ROLE, 使得 $P_{p[i]}^i$, $P_{o[j]}^i$ 不能同时赋予 role[k] ,则称 $P_{o[i]}^i$, $P_{o[j]}^i$ 是第 i 个页面功能层下的互斥操作层权限,记为 $P_{o[i]}^i \perp P_{o[j]}^i$。

由于系统权限分为了三层,因而对角色 - 权限指派也相应地分为了三层。

定义 7 $P_F \subseteq P_F \times$ROLE 为系统功能层权限与角色之间的关系。

定义8 $P_P \subseteq P_P \times$ROLE 为页面层权限与角色之间的关系。

定义9 $P_O \subseteq P_O \times$ROLE 为操作层权限与角色之间的关系。

上述三个定义表明了系统中由于权限的分层,引起了角色需要和不同层之间权限进行指派。在进行权限和角色指派时需要考虑定义 6 的互斥权限。

1.5 用户 - 角色指派

用户 - 角色指派的作用是将用户指派到合适的角色中去。一个用户可指派多个角色。

定义 10 对于角色 role[i], role[j], 若 $\forall$ user[k] $\in$ USER, 使得 role[i] , role[j] 不能同时赋予 user[k] , 则称 role[i] , role[j] 时互斥角色,记为 role[i] $\perp$ role[j] 。

如上面的操作员和签字人员就是互斥的。操作员只有填写操作票、工作票的权限,而没有签字的权限,因而这两个角色不能由同一个用户担当。可表示为 user$\perp$ sig, 其他有 user$\perp$ sec, monitor$\perp$ sig, monitor$\perp$ sec 等。

1.6 其他约束

对 RBAC 的约束来说,除了权限互斥和角色互斥外,还存在如角色基数、权限基数、权限之间的相互依赖、角色之间的相互依赖等问题。在本系统中,由于引起安全问题的主要因素是权限之间和角色之间的互斥关系,为简化安全管理,上述几种约束关系未加以考虑。作为系统进一步完善和实施更严格的权限控制,可在以后的建设中加以实施。

2 系统实现

2.1 主要表关系

图 1 给出了与权限控制相关的表之间的关系。关系表在 Sybase 11.5 中实现。

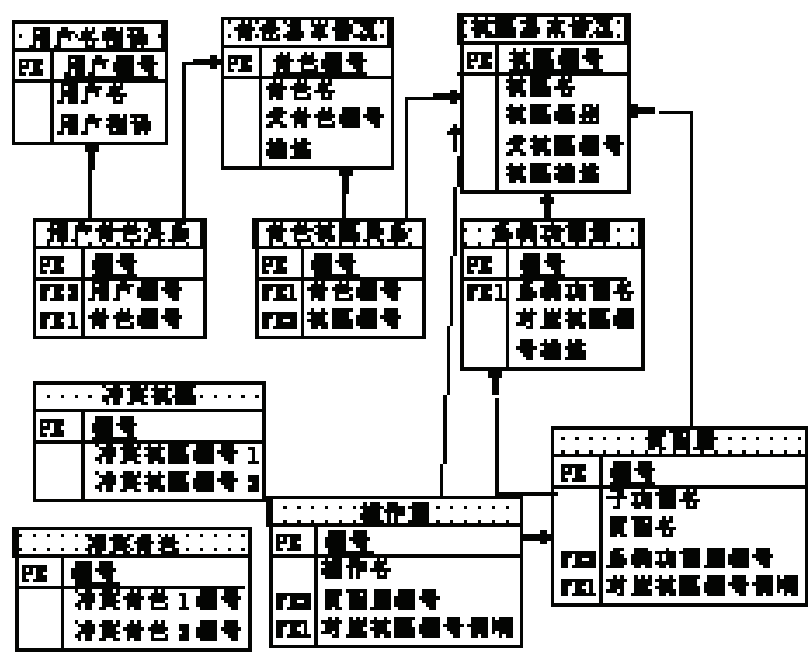


图 1 主要表之间的关系

2.2 重要流程

(1) 角色 - 权限指派(图 2)

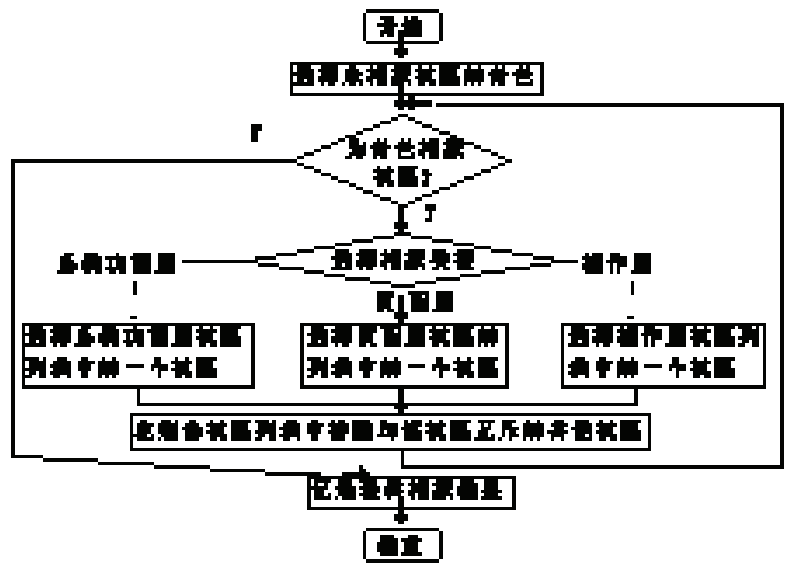


图 2 角色 - 权限指派

角色 - 权限的指派按照权限的多粒度划分, 分为三种类型, 在指派过程中考虑了权限之间的互斥关系。

权限之间的互斥关系在本系统中可表现为: ①系统功能层。对安全员 sec 来说, 其职责是检查和考核工作人员的工作业绩, 因而就不能同时具有运行记录和安全质量考核两个系统功能权限。②页面层。如系统功能层操作票管理下可分为操作票填写、操作票签字、操作票审核等页面层功能。上面三个页面层权限都是互斥的, 显然不能指派给同一个角色。③操作层。操作层常见的权限是添加、修改、删除等。显然, 为了防止对诸如变电站运行记录随意更改, 上面三个权限就不能同时赋予一个角色。

(2) 用户 - 角色指派(图 3)

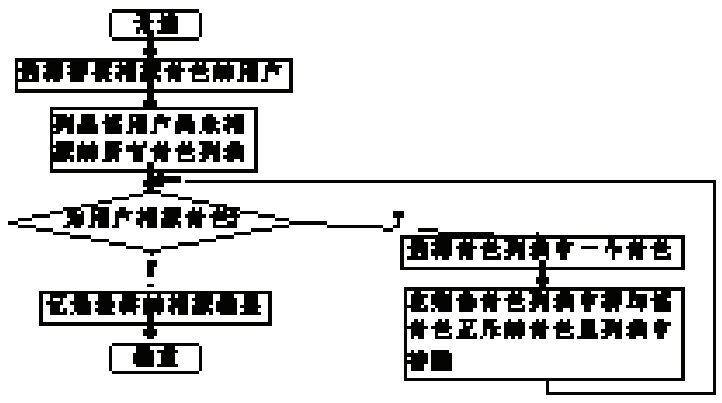


图 3　用户 - 角色指派

在指派过程中实现了角色互斥约束。

(3) 用户登录(图 4)

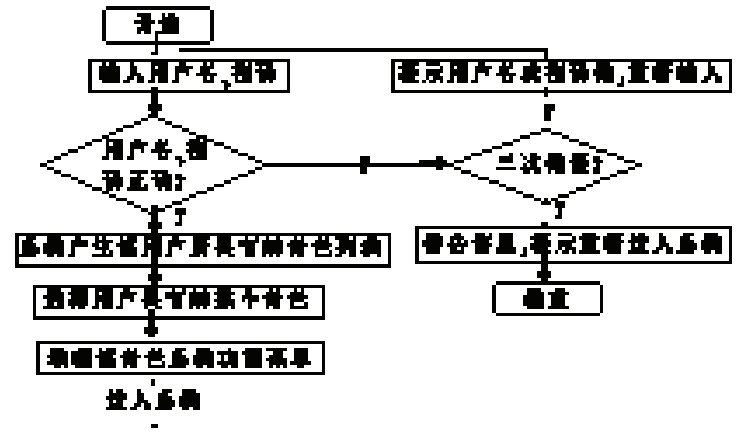


图 4　用户登录

权限管理有一个很重要的原则, 即最小权限原则。在本系统中, 为体现最小权限原则, 用户在登录系统时只能有确定的一个角色身份。这样, 用户进入系统后就只拥有该角色所有的权限。假设用户拥有操作员角色 user 和数据维护角色 dm。只考虑系统功能层, 则当用户以 user 角色进入系统后, 就只有角色 user 所具有的所有权限, 就不能进行对基础数据的维护。而当用户以数据维护员的角色进入系统后, 就只能进行基础数据的维护, 不能对系统的运行数据等进行操作。

为了用户使用方便, 本系统采用了统一的用户名和登录名, 即一个用户在系统中只有一个用户名和密码, 用户通过选择不同的角色进入系统, 拥有不同角色的权限。避免了常见的用户拥有的多个用户名和密码时容易遗忘的问题。

3　结束语

我们在变电站管理系统中应用了本文介绍的方法。实践表明, 对权限进行多粒度划分和控制后, 一方面系统管理人员的管理负担减轻; 另一方面达到了灵活控制用户权限的目的, 很好地满足了实际应用需求。

参考文献:

[1]　avi S Sandhu, et al. Role- Based Access Control Models[J] . IEEE Computer, 1996, 29(2) : 38-47.

[2]　Ravi S Sandhu, et al. The ARBAC97 Model for Role- based Administration of Roles[J] . TISSEC, 1999, 2(1) : 105-135.

[3]　陈林, 阳富民, 胡贯荣. 基于角色的多级访问控制模型[J] . 华中科技大学学报(自然科学版) , 2002, 30(2) : 102-104.

[4]　胡和平, 邹松. 角色互斥在角色访问控制系统中的应用[J] . 计算机工程, 2002, 28(4) : 124-126.

作者简介:

叶春晓(1973-) , 男, 讲师, 博士研究生, 主要研究方向为网络安全、数据库技术; 符云清, 男, 副教授, 博士, 主要研究方向为网络安全、现代远程教育技术; 吴中福, 男, 博士生导师, 主要研究方向为网络安全; 李云, 男, 博士研究生, 主要研究方向为网络安全、图像识别。

(上接第 47 页)

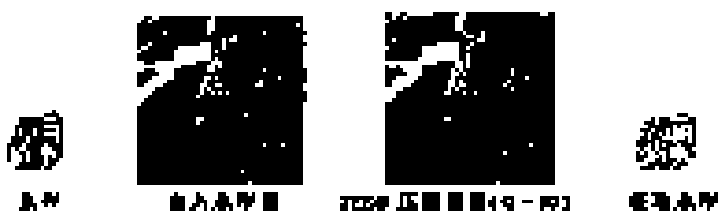


图 3　数字水印抗 JPEG 压缩实验

4　结论

本文提出了一项用于数字图像版权保护的数字水印方案。采用该方案, 原始图像与嵌入水印的图像的区别从人的感官上是不可分辨的, 图像的主观和客观效果都很好。与现有 DCT 水印技术相比, 该水印方案具有更高的图像质量(采用整数 DCT 变换和引入视觉模型) , 同时还有更高的安全性(基于单向 Hash 函数) 。

参考文献:

[1]　C Chang, T C Wu. Remote Password Authentication with Smart Cards[J] . IEE Proceedings- E, 1991, 138(3) : 165-168.

[2]　G Voyatzis, Ipitas. The Use of Watermarks in Protection of Digital Multimedia Products[J] . Proceedings of IEEE, 1999, 87(7) : 1197-1207.

[3]　R C Merkle. One-way Hash Functions and DES[C] . Advances in Cryptology, CRYPTO '89, Lecture Notes in Computer Science, vol. 435, 1989. 428-466.

[4]　R Ohbuchi, et al. Watermarking Three- dimensional Polygoal Models through Geometric and Topological Modifications[J] . IEEE Journal on Selected Areas in Communications, 1998, 16(4) : 551-560.

[5]　L Z Cheng, X Hu, Y Luo. Integer Discrete Cosine Transform and Its Fast Algorithm[J] . Electronics Letters, 2001, 37(1) : 64-65.

[6]　Y Zeng, et al. Integer Discrete Cosine Transform and Fast Algorithms [J] . IEEE Trans. Signal Processing, 2001, 49(11) : 2774-2782.

[7]　M O Rabin. Digitalized Signatures and Public-key Functions as Intractable as Factorization[R] . Technical Report MIT/LCS/TR - 212, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge Mass., 1990.

[8]　刘宇新, 李衍达. 基于重叠正交变换的自适应图像水印[J] . 电子学报, 2001, 29: 1368-1372.

[9]　刘振华, 尹萍. 信息隐藏技术及其应用[M] . 北京: 科学出版社, 2002.

作者简介:

舒世昌(1962-) , 长沙人, 讲师, 国防科大在职研究生, 研究方向为计算数学。