ISSN1000-9825 Journal of Software 软件学报 2000,11(6):779~784

扩充角色层次关系模型及其应用*

钟华[1,2] 冯玉琳[1,2] 姜洪安[3]

[1](中国科学院软件研究所对象技术中心 北京 100080)

[2](中国科学院软件研究所计算机科学开放研究实验室 北京 100080)

[3](中国石油化工集团公司信息中心 北京 100029)

E-mail: zhongh@orcaix.iscas.ac.cn

摘要 基于网络的大规模软件应用系统面临着日益复杂的数据资源安全管理的难题.基于角色的访问控制方法(role-based access control,简称RBAC)实现用户与访问权限的逻辑分离和构造角色之间的层次关系,从而方便了数据的安全管理.该文在RBAC96模型的基础上,对角色之间的层次关系进行了扩充,定义了角色的公共权限和私有权限,引入了一般继承和扩展继承机制,形成了一个能描述复杂层次关系的角色访问控制模型EHRBAC(extended hierarchy role-based access control).同时,应用该模型完成了石化市场信息数据库系统的安全管理.EHRBAC模型可以简化角色层次关系,描述复杂的角色继承场景,并通过区分公共权限和私有权限来进一步实现最少权限原则.

关键词 角色,基于角色访问控制,继承,层次关系.

中图法分类号 TP311

随着计算机技术,特别是网络技术的发展,大型网络应用系统或数据管理系统所面临的一个难题就是日益复杂的数据资源的安全管理.常用的自主访问控制(discretionary access controls)和强制访问控制(mandatory access controls)方法都是由主体和访问权限直接发生关系,根据主体/客体的所属关系或主体/客体的安全级来决定主体是否有对客体的访问权.但是,处于全球网络环境中的计算机或软件系统的访问用户往往种类繁多、数量巨大,并且动态变化,使得用传统的访问控制方法进行安全管理变得非常困难.

基于角色访问控制RBAC(role-based access control)方法引入角色这个中介,安全管理人员根据需要定义各种角色,并设置合适的访问权限,而用户根据其责任和资历再被指派为不同的角色[1].这样,整个访问控制过程就分成了两部分,即访问权限与角色相关联,角色再与用户相关联,从而实现了用户与访问权限的逻辑分离,如图1所示,角色可以看成是一个表达访问控制策略的语义结构,它可以表示承担特定工作的资格,如外科医生、药剂师等,也可以体现某种权利与责任,如护士长、值班医生等.

①用户,②角色,③访问权限.

Fig.1 The central notion of RBAC

图1 基于角色访问控制的基本思想

由于实现了用户与访问权限的逻辑分离,基于角色的策略极大地方便了权限管理.例如,如果一个用户的职位或任务发生变化,只要将用户当前的角色去掉,加入代表新的职务或任务的角色即可.研究表明,角色/权限之间的变化比角色/用户关系之间的变化相对要慢得多,并且委派用户到角色不需要很多技术,可以由行政管理人员来执行,而配置权限到角色的工作比较复杂,需要一定的技术,可以由专门的技术人员来承

* 本文研究得到国家"九五"重点科技攻关项目基金(No.97-567),国家863高科技项目基金(No.863-306-ZD02-01-1)和国家自然科学基金(No.69883030)资助.作者钟华,1971年生,博士,主要研究领域为软件工程,分布数据资源管理.冯玉琳,1942年生,研究员,博士生导师,主要研究领域为软件工程,网络分布计算,组合软件理论.姜洪安,1963年生,高级工程师,主要研究领域为石油化工市场信息分析.

本文通讯联系人:钟华,北京 100080,中国科学院软件研究所对象技术中心

本文1999-03-16收到原稿,1999-06-07收到修改稿

担,但是不给他们委派用户的权限,这与现实中的情况正好一致.除了方便权限管理之外,基于角色的访问控制方法还可以很好地描述角色层次关系、实现最少权限原则和职责分离原则[2].

在商业应用方面,基于角色机制的安全管理已经成功地应用于很多现代网络操作系统(如 Novell 公司的 Netware 和 Microsoft 公司的 Windows NT)和大型数据库管理系统(如 Oracle 8.0,Sybase 11.5 和 INFORMIX 7.2 等)中[3].

本文主要研究基于角色访问控制中的角色层次关系模型,本文第 1 节介绍相关的工作和问题的由来.第 2 节讨论扩充层次关系的访问控制模型 EHRBAC(extended hierarchy role-based access control).第 3 节给出 EHRBAC 模型在石油化工市场信息数据库系统中的应用.最后对文章进行总结.

1 基于角色访问控制的 RBAC96 模型

基于角色的访问控制是由美国国家标准化和技术委员会(NIST)的 Ferraiolo 等人在 90 年代初提出来的[1].此后,NIST 专门成立了 RBAC 研究机构,对基于角色的访问控制进行了系统的研究与应用.Sandhu 等人在对 RBAC 进行深入研究的基础上,在 1996 年提出了一个基于角色的访问控制参考模型,即 RBAC96 模型[4,5].

RBAC96 模型包括 4 个不同层次,RBAC0 模型定义了支持基于角色访问控制的最小需求,如用户、角色、权限、会话等概念;RBAC1 模型在 RBAC0 的基础上加入了角色继承关系,可以根据组织内部权力和责任的结构来构造角色与角色之间的层次关系;RBAC2 模型在 RBAC0 的基础上加入了各种用户与角色之间、权限与角色之间以及角色与角色之间的约束关系,如角色互斥、角色最大成员数、前提角色、前提权限等;而 RBAC3 模型是对 RBAC1 和 RBAC2 的集成,它不仅包括角色的层次关系,还包括约束关系.

基于角色访问控制方法的优点在于引入了角色继承关系.当一个角色 R_1 继承另一个角色 R_2 时,R_1 就自动拥有了 R_2 的访问权限.角色继承关系自然地反映了一个组织内部的权利和责任关系(例如,外科医生继承了医生的所有权限,而首席外科医生又继承了外科医生的所有权限等),为方便权限管理提供了帮助.

但是在有些情况下,角色之间并不希望继承全部权限,如在一个课题中,每一个课题成员都有一些内部的数据资料,如临时文档等,只供课题成员自身访问,即使是对于课题负责人,也不希望他能得到.在 RBAC96 模型中,要阻塞某些权限的继承,是通过私有角色(private roles)来实现的,即如果一个角色 R_1 的部分权限不希望被另一个角色 R_2 继承,那么 R_1 必须将这些权限分离出来,派生出一个新的角色 R'_1,称为 R_1 的私有角色.在 R_1 中只能描述可以被 R_2 继承的权限,而 R'_1 中再补充描述 R_1 的私有权限.

例如,一个项目包含 4 个任务 T_1,T_2,T_3 和 T_4,其中 T_1 和 T_2 构成一个子项目,我们用 P_1 来表示参与这个子项目的成员角色,S_1 表示这个子项目的主管角色,T_1 表示参与任务 T_1 的成员角色,T_2 表示参与任务 T_2 的成员角色;T_3 和 T_4 构成另一个子子项目.同样地,我们用 P_3 表示参与这个子项目的成员角色,S_3 表示这个子项目的主管角色,T_3 表示参与任务 T_3 的成员角色,T_4 表示参与任务 T_4 的成员角色.另外,P 表示整个项目的成员角色,S 表示整个项目的主管角色.按照 RBAC96 模型,子项目的所有角色都必须派生出一个私有角色,定义子项目内部的私有权限.图 2 即为使用 RBAC96 模型构造的角色关系图.

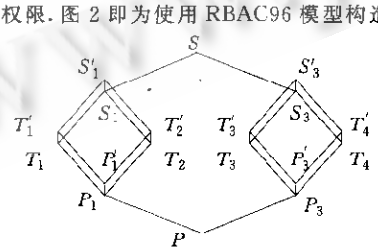

Fig. 2 An example of role inheritance hierarchy described by RBAC96
图2 RBAC96模型描述的角色层次关系图示例

这种方法最大的缺点是,将一个逻辑上统一的、属于同一角色的权限分离开来,使得很多角色(如 T_1,T_2,P_1,S_1)成为不完整的角色,只是为了继承而存在,并没有实际的物理意义.另外,私有角色的方法也使得继承关系特别复杂,从上面这个例子就可以明显地体现出来,这样,很难适应描述复杂的角色层次关系的状况.

为此,本文对 RBAC96 模型中的角色层次关系进行了扩充,定义了角色的公共权限和私有权限,并引入一般继承和扩展继承机制,形成了 EHRBAC 模型,很好地解决了使用私有角色所出现的问题.

2 扩充角色层次关系模型 EHRBAC

定义 1(用户). 用户就是一个可以独立访问计算机系统中的数据或用数据表示的其他资源的主体. 我们用 *USERS* 表示一个用户集合.

用户在一般情况下是指人,但有时也包括计算机或一些具有自治性的软件系统,如 Agent.

定义 2(权限). 权限是对计算机系统中的数据或用数据表示的其他资源进行访问的许可. 我们用 *PERMISSION* 表示一个权限集合.

基于角色的访问控制方法是策略中立的,可以看成是访问控制管理中的一个独立部件,它没有具体定义如何进行权限定义,可以使用特殊的方法,也可以直接使用强制访问控制或自主访问控制等方法.

定义 3(角色). 角色是指一个组织或任务中的工作或位置,它代表了一种资格、权利和责任. 我们用 *ROLES* 表示一个角色集合.

基于角色访问控制方法的思想就是把对用户的授权分成两部分,用角色来充当用户行使权限的中介. 这样,用户与角色之间以及角色与权限之间就形成了两个多对多的关系. 一个用户可以是很多角色的成员,一个角色也可以有多个用户. 同样地,一个角色可以有多个权限,而一个权限也可以重复配置于多个角色. 我们称这两个关系为用户委派和权限配置.

定义 4(用户委派). 用户委派是 $USERS$ 与 $ROLES$ 之间的一个二元关系,假定 $UA \subseteq USERS \times ROLES$ 是一个用户委派关系集合,那么 $(u,r) \in UA$ 表示用户 u 被委派了一个角色 r.

定义 5(权限配置). 权限配置是 $ROLES$ 与 $PERMISSION$ 之间的一个二元关系,假定 $PA \subseteq ROLES \times PERMISSION$ 是一个权限配置关系集合,那么 $(r,p) \in PA$ 表示角色 r 拥有一个权限 p.

为了实现角色权限的部分继承,我们将角色所拥有的权限划分为公共权限和私有权限两种. 其实这种划分也是很符合客观实际的,因为作为一个独立的角色,往往有一些这个角色所特有的权限.

定义 6. 令 $CP: ROLES \rightarrow 2^{PERMISSION}$, $CP(r)$ 为角色 r 所拥有的公共权限集合.

定义 7. 令 $PP: ROLES \rightarrow 2^{PERMISSION}$, $PP(r)$ 为角色 r 所拥有的私有权限集合.

由于将权限划分为公共权限和私有权限,所以我们可以引入两种继承机制:一般继承和扩展继承. 一般继承只能继承角色的公共权限,而不能继承私有权限,并且它继承下来的公共权限还是公共权限.

定义 8(一般继承). 一般继承定义了 $ROLES$ 与 $ROLES$ 之间的一个二元关系,假定 $NI \subseteq ROLES \times ROLES$ 是一个一般继承关系集合,那么 $(r_1,r_2) \in NI$ 表示角色 r_2 一般继承角色 r_1,符号表示为 $r_1 \rightarrow r_2$. 如果 $r_1 \rightarrow r_2$,那么对于 $\forall p \in CP(r_1)$,有 $p \in CP(r_2)$.

与一般继承不同的是,扩展继承不但能继承公共权限,还能继承私有权限. 继承过来的权限属性仍保持不变.

定义 9(扩展继承). 扩展继承定义了 $ROLES$ 与 $ROLES$ 之间的一个二元关系,假定 $EI \subseteq ROLES \times ROLES$ 是一个扩展继承关系集合,那么 $(r_1,r_2) \in EI$ 表示角色 r_2 扩展继承角色 r_1,符号表示为 $r_1 \bullet\!\!\rightarrow r_2$. 如果 $r_1 \bullet\!\!\rightarrow r_2$,那么对于 $\forall p \in CP(r_1)$,有 $p \in CP(r_2)$,对于 $\forall p \in PP(r_1)$,有 $p \in PP(r_2)$.

角色之间的一般继承和扩展继承关系可以构成复杂的角色层次关系图,为此,我们引入另外几个关系.

定义 10. 关系 $\rightarrow^+$ 定义为:如果 $r_a \rightarrow^+ r_b$,那么存在 $r_1, r_2, \ldots, r_n \in ROLES$(其中 $n>0$),使得 $r_a \rightarrow r_1, r_1 \rightarrow r_2, \ldots, r_n \rightarrow r_b$.

定义 11. 关系 $\rightarrow^*$ 定义为:如果 $r_a \rightarrow^* r_b$,那么有 $r_a \rightarrow r_b$ 或 $r_a \rightarrow^+ r_b$,称为 r_b 弱一般继承 r_a.

定义 12. 关系 $\bullet\!\!\rightarrow^+$ 定义为:如果 $r_a \bullet\!\!\rightarrow^+ r_b$,那么存在 $r_1, r_2, \ldots, r_n \in ROLES$(其中 $n>0$),使得 $r_a \bullet\!\!\rightarrow r_1, r_1 \bullet\!\!\rightarrow r_2, \ldots, r_n \bullet\!\!\rightarrow r_b$.

定义 13. 关系 $\bullet\!\!\rightarrow^*$ 定义为:如果 $r_a \bullet\!\!\rightarrow^* r_b$,那么有 $r_a \bullet\!\!\rightarrow r_b$ 或 $r_a \bullet\!\!\rightarrow^+ r_b$,称为 r_b 弱扩展继承 r_a.

从以上的定义不难得到下面的几条定理.

定理 1. $r_1 \rightarrow^* r_2$,那么对于 $\forall p \in CP(r_1)$,有 $p \in CP(r_2)$.

定理 2. 如果 $r_1 \bullet\!\!\rightarrow^* r_2$,那么对于 $\forall p \in CP(r_1)$,有 $p \in CP(r_2)$.

定理 3. 如果 $r_1 \bullet \rightarrow^* r_2$,那么对于$\forall\ p \in PP(r_1)$,有 $p \in PP(r_2)$.

根据定理 1～3,我们可以得到判定一个角色是否拥有某个私有权限(公共权限)的方法,即只要查找自身和所有被其弱一般继承(弱扩展继承)的角色是否拥有这个私有权限(公共权限).

为了直观地表示角色层次关系,我们用一个矩形来表示角色,内部标有角色名称;用一个单线箭头表示角色的一般继承关系,其中箭头从被继承角色指向继承角色,如图 3(a)所示;用一个虚线箭头表示扩展继承关系.同样地,箭头从被继承角色指向继承角色,如图 3(b)所示.

这样,前面那个例子用 EHRBAC 就可以表示成图 4 的形式.可以看出,EHRBAC 模型可以简化角色层次关系,描述复杂的角色继承场景.另外,通过区分公共权限和私有权限还可以进一步达到最少权限原则,使得对于每一个角色,只需将它完成任务所必须的权限配置给它,防止用户滥用职权,减少用户由于疏忽而可能对系统造成的危害.

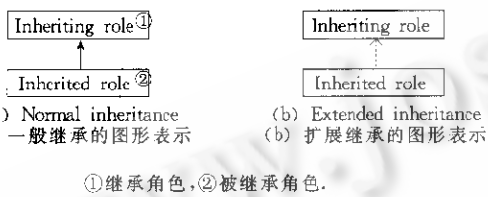

Fig. 3 Diagrammatic representation of normal inheritance and extended inheritance
图3 一般继承和扩展继承的图形表示

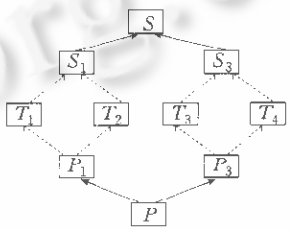

Fig. 4 An example of role inheritance hierarchy described by EHRBAC
图4 EHRBAC模型描述的角色层次关系图示例

3 EHRBAC 应用

中国石油化工集团公司信息中心的石化市场信息数据库系统是一个大型的分布数据资源管理系统,它包括国际石化市场信息、石化产品进出口信息、国内石化产品市场信息、石化市场全文检索信息等等.访问此系统的用户不仅包括石化总公司的职员,还包括其下属企业和工厂,甚至是一般的 Internet 用户,再加上信息种类繁多、信息量巨大以及不同程度的信息敏感度,使得其安全管理非常复杂.

我们使用前面描述的 EHRBAC 模型实现了它的安全管理.根据其安全需求,我们定义了一个详细的角色层次关系图,并提供辅助工具来动态生成新的角色和维护角色层次关系.图 5 为其角色层次关系图中有关信息分析领域的一部分,并未包括生产、销售、计划等领域,所以实际应用中的角色数和角色关系要复杂得多.

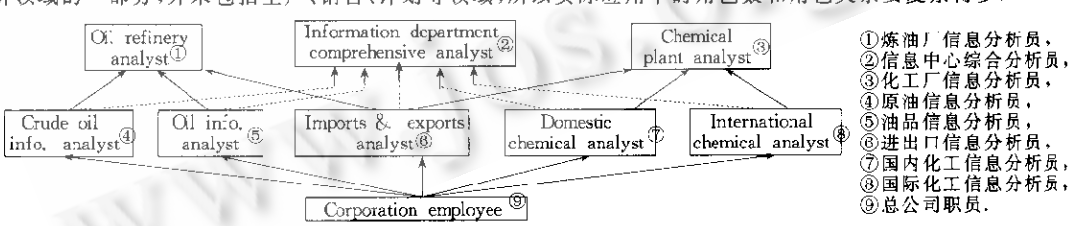

Fig. 5 Role hierarchy in the petrochemical market information system (the field of information analyzing)
图5 石化市场信息角色层次关系图(信息分析领域)

在应用中,权限用一个二元组(数据对象,访问类型)来表示,如(*InterCrudeOil*,*S*)表示可以查询国际原油信息.权限信息和继承关系都作为属性存放在角色中,并使用一个角色描述语言 RDL 来进行定义和管理,下面是角色描述语言 RDL 的规范.

```
〈Role Specification〉 ::=Role 〈Role Name〉
                          {
                            〈Normal Inheritance〉; //定义一般继承关系
                            〈Extended Inheritance〉; //定义扩展继承关系
                            〈Common Permissions〉; //定义公共权限
```

```
                    〈Private Permissions〉; //定义私有权限
                }
〈Normal Inheritance〉    ::=Normal Inheritance:〈Role Names〉
                    |φ
〈Extended Inheritance〉  ::=Extended Inheritance:〈Role Names〉
                    |φ
〈Common Permissions〉    ::=Common Permissions:〈permissions〉
                    |φ
〈Private Permissions〉   ::=Private Permissions:〈permissions〉
                    |φ
〈Permissions〉           ::=〈Permission〉 〈Permission〉,〈Permissions〉
〈Permission〉            ::=(
                        〈Category〉,
                        〈Access Mode〉
                    )
〈Role Names〉            ::=〈Role Name〉
                        |〈Role Name〉,〈Role Names〉
〈Role Name〉             ::=〈Chars〉
〈Category〉              ::=〈Chars〉
〈Access Mode〉           ::=S|U|D|I E
〈Chars〉                 ::=〈Char〉
                        |〈Char〉〈Chars〉
〈Char〉                  ::=A|B|...|Z|a|b|...|z|0|1|...|9|_|#
```

下面是原油信息分析员和信息中心综合分析员用 RDL 语言描述的详细信息,为了方便理解,角色名和数据对象都用中文表示:

```
Role 原油信息分析员{
  Normal inheritance:总公司职员;
  Common permission:
      〈国际原油市场信息,S〉,
      〈每日油价快报,S〉;
}
```

```
Role 信息中心综合分析员{
  Extended inheritance:原油信息分析员,
                       油品信息分析员,
                       国际化工信息分析员,
                       国内化工信息分析员,
                       进出口信息分析员;
  Common permission:
    〈中石化信息快讯,S〉;
  Private permission:
    〈石化市场分析参考,S〉;
}
```

4 结 论

基于网络的大规模软件应用系统面临着日益复杂的数据资源安全管理的难题.基于角色的访问控制方法实现了用户与访问权限的逻辑分离和构造角色之间的层次关系,方便了数据安全管理.为了克服使用私有角色所带来的问题,本文在 RBAC96 模型的基础上,对角色之间的层次关系进行了扩充,定义了角色的公共权限和私有权限,引入了一般继承和扩展继承机制,形成了一个扩充层次关系的角色访问控制模型 EHRBAC,并应用该模型实现了石化市场信息数据库系统的安全管理.进一步的研究工作是在 EHRBAC 模型的基础上,融入角色的约束关系和合作关系,形成一个完整的扩充角色层次关系模型.

参考文献

1 Ferraiolo D F, Kuhn R. Role-Based access control. In: Proceedings of the 15th National Computer Security Conference. Baltimore, MD, 1992. 554~563, http://hissa.ncsl.nist.gov/kuhr/

2 Sandhu R, Samarati P. Access control: principles and practice. IEEE Communications, 1994,32(9):40~48
3 Ramaswamy C, Sandhu R. Role-Based access control features in commercial database management systems. In: Proceedings of the 21st National Information Systems Security Conference. Virginia: U. S. Government Printing Office, 1998, http://www.list.gmu.edu/conferen.htm
4 Sandhu R, Coyne E J, Feinstein H L *et al.* Role-Based access control models. IEEE Computers, 1996,29(2):38~47
5 Sandhu R. Rationale for the RBAC96 family of access control models. In: Proceedings of the 1st ACM Workshop on Role-Based Access Control. ACM, 1997. http://www.list.gmu.edu/conferen.htm

A Role Hierarchy Model for Role-Based Access Control and Its Application

ZHONG Hua[1,2] FENG Yu-lin[1,2] JIANG Hong-an[1]

[1](*Object Technology Center Institute of Software The Chinese Academy of Sciences Beijing* 100080)
[2](*Laboratory for Computer Science Institute of Software The Chinese Academy of Sciences Beijing* 100080)
[3](*Information Department China Petrochemical Corporation Beijing* 100029)

Abstract One of the most challenging problems in managing large computer software systems on global network is the complexity of security administration. The RBAC (role-based access control) method shows powerful capability on access control by realizing logical separation between users and permissions and constructing role hierarchies. This paper presents a role hierarchy model EHRBAC (extended hierarchy role-based access control) based on RBAC96, which defines common permissions and private permissions and imports normal inheritance and extended inheritance. Based on EHRBAC, the authors realize the security administration for the Petrochemical Market Information System. The EHRBAC model can specify the complex inheritance of roles and simplify their relation hierarchies. It minimizes the role access permissions by the separation of private permissions from common permissions.

Key words Role, role-based access control, inheritance, hierarchy.