基于映射机制的细粒度 RBAC 委托授权模型

蔡伟鸿[1,2],韦 岗[1],肖 水[2]
(1.华南理工大学电子与信息学院,广东广州 510640;2.汕头大学计算机科学与技术系,广东汕头 515063)

摘 要: 针对现有 RBAC(Role-Based Access Control)委托授权模型存在的不足:其一,没有有效地实现细致委托粒度;其二,权限传播没有得到很好的控制,给出一种基于映射机制的细粒度角色委托模型 RDBMPM(Fine-Grained Role Delegation Model Based Permission Mapping Mechanism),该模型基于向量化与度量化算子的复合运算,提出了度量角色的概念,并以其为授权粒度对委托约束机制进行讨论,增强了权限传播的可控性.最后,通过三个典型的支持细粒度委托的模型在映射机制下的具体实现,验证了 RDBMPM 模型的研究意义.

关键词: 访问控制; 角色委托模型; 映射机制; 度量角色
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 08-1753-06

Fine-Grained Role Delegation Model Based on Mapping Mechanism

CAI Wei-hong[1,2], WEI Gang[1], XIAO Shui[2]
(1. *School of Electronic and Information Engineering, South China University of Technology, Guangzhou, Guangdong* 510640, *China*;
2. *Department of Computer Science and Technology of Shantou University, Shantou, Guangdong* 515063, *China*)

Abstract: There are some faults in the existing role-based delegation models: (1) most of these models can rarely support a fine delegation granularity effectively; (2) the propagation of permissions in them is poorly-controlled. This paper analyzed these problems, and proposed a fine-grained role delegation model based on mapping mechanism (RDBMPM), which mainly consisted of a vectorizing operator and a measuring operator. Based on these two operators' concerted computing, the paper introduced the concept of measuring role, which acts as the authorized granularity in the following discussion of delegation constraint mechanism. Finally the significance of the research on RBAC(Role-Based Access Control) delegation model based on mapping mechanism is justified by the simulating of three typical fine-grained delegation models in RDBMPM.

Key words: access control; role based delegation model; mapping mechanism; measuring role

1 引言

基于角色的访问控制模型正越来越受到重视[1,2].它是一种结合了自主访问控制和强制访问控制各自优点的访问控制方法,尤其以 Sandhu 提出的 RBAC96 模型最为著名,该模型得到了美国国家标准技术研究所的支持.

角色委托授权模型是近几年 RBAC 领域的一个研究热点.在大型分布式系统中,一方面如果完全依赖于集中式授权,将使系统管理者的工作异常繁重;另一方面普通用户希望在符合系统安全规定的情况下自主地把一些权限委托给其他用户.基于角色的委托模型正是针对上述需求而提出的.目前,委托粒度和约束的研究是 RBAC 委托模型的研究重点.在实际应用情况下,委托机制仅支持整个角色是不恰当的,因为安全策略通常要求用户只能委托角色的部分权限.

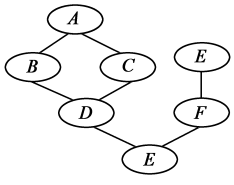
本文通过研究细粒度 RBAC 授权许可之间的关系,提出了一种基于映射机制的细粒度 RBAC 委托模型 RDBMPM (Fine-Grained Role Delegation Model Based Permission Mapping Mechanism),该模型从构造角色委托需求集到唯一标识符集的映射机制出发,基于向量化与度量化算子提出了度量角色的概念,委托模型将基于度量角色来实现细粒度委托.为增强在委托过程中的可控性,本文也对模型的委托约束机制进行了相关研究.本文最后给出模型的具体应用,验证了映射机制对于细粒度 RBAC 委托的研究意义.

收稿日期:2009-07-30;修回日期:2009-12-12
基金项目:国家自然科学基金-国家杰出青年科学基金(No.60625101);广东省现代信息服务业发展专项(No.GDIID2008IS046);省部产学研合作项目(No.2009B090300345)

2 相关工作

最早提出 RBAC 环境下的委托模型的是 Sandhu 和 Barka,他们分析与总结了角色委托模型的基本特性[3],包括委托的单调性、委托粒度等.$RBDM_0$[4]是 Barka 等人提出的仅支持扁平角色和单步委托的模型.$RBDM_1$[5]是 $RBDM_0$ 的扩展,它支持角色层次,但仍不支持多步和部分委托.文献[6]中提出了 RDM2000,该模型是基于委托树来支持角色层次下的多步委托.

RBDM 和 RDM2000 都属于委托粒度为角色级别的模型,即一旦将某个角色转授出去,就必须将其所包含的全部权限都委托出去.在实际应用中,这一点违背授权管理的"最小特权"原则.例如,在图 1 所示的 RBAC 模型中,角色 A 的用户 John 可能只希望把 p_1 委托给角色 D 的用户 Jenny,而不希望把 p_2 也委托给他.对部分委托的不支持,大大影响了这两类模型在应用中的灵活性.为克服这方面的不足,Zhang[7]等人提出了 PBDM,该模型支持角色和部分委托,其中部分委托是通过临时角色来实现的.这种方法需创建大量的临时角色,导致模型管理严重复杂化.



Role hierarchy

UA

角色	用户
A	John
B	Tom
C	Smith
D	Jenny
E	Scott

UA

角色	权限
A	p_1,p_2
B	p_3
C	p_4,p_5
D	p_6
E	p_7

图1 RBAC委托模型示例

文献[8]和[9]分别在分析"委托权利"与"委托关系"的基础上提出了对系统权限进行委托的方法,然而它们只支持权限级别的委托.文献[10]给出了一种支持重复和部分角色的委托模型 RPRDM,该模型基于屏蔽值的概念,可以指定哪些权限被委托出去.文献[11]提出采用量化角色来实现灵活委托.但屏蔽值机制和量化角色都过于简单,它们在委托过程中只能决定某一权限是否包含在委托角色中,而不能对其授权使用次数进行控制,不具有实际委托需求的普遍性.这是因为,在层次 RBAC 中,角色继承关系通常引起权限之间的地位形成等级性.例如,在图 1 中,角色 A 可继承 B 的权限 p_3,假设 John 把其角色 A 的 p_1 和 p_3 委托给 Tom,出于系统安全性与主观需要,系统或委托人认为 p_1 比 p_3 的委托要求等级要高,因此,John 只希望把角色 A 的 p_1 的 1 次使用权与 p_3 的 3 次使用权转授给 Tom.这种在同一次部分委托时,因 RBAC 系统的权限等级性所导致的委托使用次数限制的差异性是屏蔽值和量化角色所不支持的.此外,在委托约束方面,它们也不支持周期性时限的限制等.

3 RDBMPM 模型

3.1 RDBMPM 模型定义

定义 1 带使用次数限制的委托授权许可表达式 $E(R,\lambda)$

$$E(R,\lambda)=\lambda_0 p_0+\lambda_1 p_1+\cdots+\lambda_n p_n=\sum_{i=0}^{n}\lambda_i p_i=\boldsymbol{\lambda}\cdot\boldsymbol{p}^{\mathrm{T}} \tag{1}$$

其中,$\boldsymbol{\lambda}=(\lambda_0,\lambda_1\cdots,\lambda_n)$,$\boldsymbol{p}=(p_0,p_1,\cdots,p_n)$,$\lambda_i\in N$,$i=0,1,\cdots,n$.当 $\lambda_i=0$ 表示本次委托中将不包含角色 R 的权限 p_i;当 $\lambda_i\neq 0$ 表示本次委托中将包含 p_i,且其受托者获得该权限的最大使用次数为 λ_i.

定义 2 授权许可向量 $\boldsymbol{V}(R,\boldsymbol{\lambda})$

记 $M(R)$为角色 R 中对应的全部 $E(R,\boldsymbol{\lambda})$所组成的用户角色委托需求集.为分析 $M(R)$中各 $E(R,\boldsymbol{\lambda})$之间的关系,本文引入授权许可向量的概念.对于任意 $E(R,\boldsymbol{\lambda})$,可通过对其进行矢量化(矢量化算子记为 Vector)后得到相应的授权许可向量,其定义如式(2)所示.

$$\boldsymbol{V}(R,\lambda)=\mathrm{Vector}(E(R,\lambda))=\mathrm{Vector}(\sum_{i=0}^{n}\lambda_i\cdot p_i)=\boldsymbol{\lambda}=(\lambda_0,\lambda_1,\cdots,\lambda_n) \tag{2}$$

由式(2)知,$\boldsymbol{V}(R,\lambda)$与 $E(R,\lambda)$是一一对应的,即由一个 $E(R,\lambda)$通过 Vector 后可唯一得 $\boldsymbol{V}(R,\lambda)$,反之,$\boldsymbol{V}(R,\lambda)$经 Vector 的逆操作 Vector-1 也可得唯一的 $E(R,\lambda)$.

定义 3 授权许可关系"$\subset$","$\not\subset$"

①授权许可可达关系"$\subset$"

$E(R,\boldsymbol{\lambda}')\subset E(R,\boldsymbol{\lambda})\Leftrightarrow\boldsymbol{V}(R,\lambda')\subset\boldsymbol{V}(R,\lambda)\Leftrightarrow\exists_{\boldsymbol{\alpha}\in N^{n+1}}\boldsymbol{\alpha}\cdot\mathrm{diag}(\boldsymbol{\lambda})\geqslant\boldsymbol{\lambda}'\Leftrightarrow\exists_{\alpha\in\mathbf{N}^{n+1}}\alpha_i\lambda_i\geqslant\lambda'_i$,$i=0,\cdots,n$

②授权许可不可达关系"$\not\subset$"

$E(R,\boldsymbol{\lambda}')\not\subset E(R,\boldsymbol{\lambda})\Leftrightarrow V(R,\boldsymbol{\lambda}')\not\subset V(R,\boldsymbol{\lambda})\Leftrightarrow\forall_{\alpha\in N^{n+1}}\exists_{i\in\{0,1,2\cdots,n\}}\alpha_i\lambda_i<\lambda'_i$,$i=0,\cdots,n$

当 $E(R,\boldsymbol{\lambda}')\subset E(R,\boldsymbol{\lambda})$时,表示前者所要委托权限可通过正整数次后者的委托来实现,反之,当 $E(R,\lambda')\not\subset E(R,\lambda)$时,则表示后者无论经过多少次委托操作都无法得前者所期望的委托权限.

定义 4 授权许可基组与授权许可基矩阵

令 $\boldsymbol{\gamma}=(\gamma_0,\gamma_1,\cdots,\gamma_n)$,$\boldsymbol{\lambda}=(\lambda_0,\cdots,\lambda_n)$,$\boldsymbol{\lambda}^{(i)}=(\lambda_0^{(i)},\cdots,\lambda_n^{(i)})$.

①授权许可线性相关:

$$\boldsymbol{V}(R,\boldsymbol{\lambda}^{(i)})\subset\boldsymbol{V}(R,\boldsymbol{\lambda})\vee\boldsymbol{V}(R,\boldsymbol{\lambda})\subset\boldsymbol{V}(R,\boldsymbol{\lambda}^{(i)}) \tag{3}$$

②授权许可线性无关:

$$\boldsymbol{V}(R,\boldsymbol{\lambda}^{(i)})\not\subset\boldsymbol{V}(R,\boldsymbol{\lambda})\wedge\boldsymbol{V}(R,\boldsymbol{\lambda})\not\subset V(R,\lambda^{(i)}) \tag{4}$$

③授权许可线性表出:

$$\boldsymbol{V}(R,\boldsymbol{\lambda})=\gamma_0\boldsymbol{V}(R,\boldsymbol{\lambda}^{(0)})+\cdots+\gamma_n\boldsymbol{V}(R,\boldsymbol{\lambda}^{(n)})$$

$$\text{即}\ \exists_{\gamma\in N^{n+1}}\lambda = \sum_{i=0}^{n}\gamma_i\cdot\boldsymbol{\lambda}^{(i)} \tag{5}$$

当 $\boldsymbol{V}(R,\lambda)$与 $\boldsymbol{V}(R,\lambda')$满足式(3)时,称它们是线性相关的,反之,满足式(4)则称它们是线性无关.当多个授权许可向量两两线性无关时,称它们为 $M(R)$的一个线性无关组.同样,当它们之间的关系满足式(5)时,则称 $\boldsymbol{V}(R,\boldsymbol{\lambda})$可以由组 $\boldsymbol{V}(R,\boldsymbol{\lambda}^{(i)})$线性表出.

记 $\boldsymbol{V}(R,\boldsymbol{\lambda}^{(i)})=\boldsymbol{e}_i$,当组$\{\boldsymbol{e}_i\}$同时满足如下条件 1 与 2 时,称$\{\boldsymbol{e}_i\}$为 $M(R)$的授权许可基组.将由基组$\{\boldsymbol{e}_i\}$对应的向量按列排列所构成的矩阵称为 $M(R)$的授权许可基矩阵.

条件 1:$\forall_{0\leqslant k,h\leqslant n且k\neq h},\boldsymbol{e}_k\not\subset\boldsymbol{e}_h\wedge\boldsymbol{e}_h\not\subset\boldsymbol{e}_k$

条件 2:$\forall_{\boldsymbol{v}\in\mathrm{Vector}(M(R))},\exists!_{\gamma\in N^{n+1}}\boldsymbol{v}\sum_{i=0}^{n}\gamma_i\boldsymbol{e}_i$

条件 1 表示授权许可基组中任意两个元素之间都是线性无关的;条件 2 则要求任意 $\boldsymbol{V}(R,\boldsymbol{\lambda})$都可由组$\{\boldsymbol{e}_i\}$唯一线性表出,其中符号"∃!"表示"有且仅存在一个".记矩阵 $\boldsymbol{G}=(\boldsymbol{g}_0^{\mathrm{T}},\boldsymbol{g}_1^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}})$为如下形式:$\boldsymbol{g}_0=(1,0,\cdots,0),\boldsymbol{g}_1=(0,1,0,\cdots,0),\cdots,\boldsymbol{g}_n=(0,0,\cdots,1)$.

定理 1　矩阵 $\boldsymbol{G}$ 是 $M(R)$的授权许可基矩阵.

证明:

①在 RBAC 中,由于权限是其授权的最小单位,因而它们具有原子性,故知组$\{\boldsymbol{g}_i\}$是线性无关组,满足条件 1.

②根据定义 1 和 2,当取 $\gamma_0=\lambda_0,\gamma_1=\lambda_1,\cdots,\gamma_n=\lambda_n$ 时,任意的 $\boldsymbol{V}(R,\boldsymbol{\lambda})$都可通过组$\{\boldsymbol{g}_i\}$唯一线性表出,故满足条件 2.　　证毕

定义 5　授权许可坐标 $\boldsymbol{x}$

由前讨论知,$\boldsymbol{G}$ 是 $M(R)$的授权许可基矩阵,且任意一个 $\boldsymbol{V}(R,\boldsymbol{\lambda})$都可在 G 下唯一线性表出.即

$$\boldsymbol{V}(R,\boldsymbol{\lambda})=\sum_{i=0}^{n}x_i\boldsymbol{g}_i^{\mathrm{T}}=\boldsymbol{x}\cdot\boldsymbol{G} \tag{6}$$

这里,$\boldsymbol{x}=(x_0,x_1,\cdots,x_n)$称为 $\boldsymbol{V}(R,\boldsymbol{\lambda})$在 $\boldsymbol{G}$ 下的授权许可坐标.令变换 $J(\boldsymbol{G})=\boldsymbol{G}^{-1}$.由式(6)知,$\boldsymbol{V}(R,\boldsymbol{\lambda})$经 J 作用后的像为 $\boldsymbol{x}$.同样,易知存在逆变换 $J^{-1}(\boldsymbol{G})=\boldsymbol{G}$,使得 $\boldsymbol{x}$ 经过 J^{-1}作用后的像为 $\boldsymbol{V}(R,\lambda)$.

定义 6　委托向量化算子 H

本文将实现由 $E(R,\lambda)$到 $\boldsymbol{x}$ 的这一变换过程描述为 RDBMPM 的委托向量化算子 H,即 H 的定义为:

$$H(E(R,\lambda))=J\circ\mathrm{Vector}(E(R,\lambda))=\boldsymbol{x} \tag{7}$$

上式中的"∘"为左复合关系运算(下同).因 J 与 Vector 都可逆,所以 H 是可逆的,记其逆算子为 H^{-1},易得 H^{-1}为:

$$H^{-1}(\boldsymbol{x})=\mathrm{Vector}^{-1}\circ J^{-1}(\boldsymbol{x})=E(R,\boldsymbol{\lambda}) \tag{8}$$

令 Max(R)为权限集的最大委托使用次数.记 S 为笛卡尔集 N^{n+1}到自然数集 N 的权限映射,其定义域 X 与值域 Y 的定义分别如下:$X=\mathrm{domain}(R)=\{(x_0,x_1,\cdots,x_n)\mid x_i\leqslant\mathrm{Max}(R),i=0,1,\cdots,n\}$;　$Y=\mathrm{range}(R)=\{y\mid\forall x\in X\}$.

定义 7　如果映射 $S:X\to Y$ 满足如下性质,则称 S 为 RBAC 委托度量化算子.

①$S(\boldsymbol{x})\geqslant 0,\boldsymbol{x}\in X$,当且仅当 $\boldsymbol{x}=(0,0,\cdots,0)$时,$S(\boldsymbol{x})=0$

②$S(a\boldsymbol{x})=aS(\boldsymbol{x}),a\in N$

③$S(\boldsymbol{x}+\boldsymbol{x}')=S(\boldsymbol{x})+S(\boldsymbol{x}'),\boldsymbol{x},\boldsymbol{x}'\in X$

④$S(\boldsymbol{x})\neq S(\boldsymbol{x}')$,当 $\boldsymbol{x}\neq\boldsymbol{x}'$时.即,对任意 $\boldsymbol{x}\in X$,S 存在逆映射 S^{-1},使得 $S^{-1}(S(\boldsymbol{x}))=\boldsymbol{x}$

性质 1 保证映射后的结果为非负;性质 2 与 3 称为权限映射的线性性质;性质 4 称为 RBAC 映射机制的逆操作.当用户之间基于授权序对 $<R,K>$ 进行委托时,系统先用性质 4 找到与之对应的 $\boldsymbol{x}$,再通过 $\boldsymbol{x}$ 与 $E(R,\boldsymbol{\lambda})$的关系,最终找到所期望的委托权限.

定义 8　细粒度 RBAC 委托授权映射机制

细粒度 RBAC 委托映射机制是一个映射算子 F,它由向量化算子 H 与度量化算子 S 通过复合而得到,即映射算子 F 的定义为:

$$F=S\circ H \tag{9}$$

其中,$H=J\circ\mathrm{Vector}$,$S:X\to Y$.同样,因 S 与 H 是可逆的,可得 F 的逆算子 F^{-1}为:$F^{-1}=H^{-1}\circ S^{-1}$.

在图 2 中,任意 $E(R,\boldsymbol{\lambda})$都可经 F 作用后与唯一的自然数 K 建立起对应关系,从而为不同委托权限组合分配了唯一的标识符 $<R,K>$,如步骤 step1-step6 所示.同样,由于 F 是可逆的,当委托用户提交不同的委托请求 $<R,K>$ 时,系统将按照 F^{-1}所定义的作用过程,先基于 S^{-1}将 $<R,K>$ 映射为 $\boldsymbol{x}$,再基于 H^{-1}将 $\boldsymbol{x}$ 映射为唯一的 $E(R,\boldsymbol{\lambda})$,从而实现细粒度的委托,如步

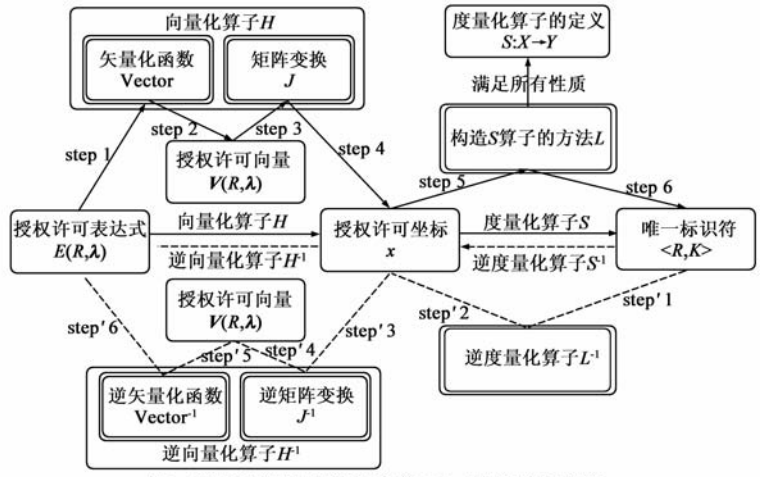


图2　基于映射机制的细粒度RBAC委托授权模型

骤 step′1 – step′6 所示.

定理 2 $L(x_0,x_1,\cdots,x_n)=x_0+x_1A+x_2A^2+\cdots+x_nA^n=\sum_{i=0}^{n}x_iA^i$ 满足是满足定义 7 的度量化算子.其中,$A\geqslant 2$,$x_i\in\{0,1,2,\cdots,A-1\}$,$i=0,1,\cdots,n$,$A-1$ 为权限集的最大授权次数,即 $A=\mathrm{Max}(R)+1$.

证明:

①显然 $L(x_0,x_1,\cdots,x_n)\geqslant 0$,所以满足性质 1.

②再证 L 具有线性性质.

$$L(\alpha\boldsymbol{x})=\alpha x_0+\alpha x_1\cdot A+\cdots\cdots+\alpha x_n\cdot A^n=\alpha L(\boldsymbol{x})$$

$$L(\boldsymbol{x}+\boldsymbol{x}')=(x_0+x'_0)+(x_1+x'_1)A+,\cdots,+(x_n+x'_n)\cdot A^n=L(x)+L(x')$$

③反证法证 L 具有性质 4.令 $M_i=A_i*\boldsymbol{x}_i$,假设存在 $L(\boldsymbol{x})=L(\boldsymbol{x}')$,且 $\boldsymbol{x}\neq\boldsymbol{x}'$,则

$$x_0+x_1A+\cdots x_iA^i+\cdots x_jA^j=x'_0+x'_1A+\cdots x'_kA^k+\cdots,x'_hA^h$$

其中,上式中的系数都大于或等于 1.在式(10)中有最大项,不妨令其为 $x_h'A^h$.

$$x'_hA^h=\mathrm{Max}(x_0,\cdots,x_iA^i,x'_0,\cdots,\cdots,x'_hA^h)\quad(11)$$

又因$\{M_i\}$前 n 项和的最大值具有如下性质:

$$\mathrm{Max}(\sum_{i=0}^{n-1}M_i)=(A-1)\frac{(1-A^n)}{1-A}<A^n\quad(12)$$

结合式(11)与(12)可得:$x'_hA^h\geqslant A^h>\mathrm{Max}\sum_{i=0}^{i=j}M_j>L(\boldsymbol{x})$

因而式(10)的假设不成立,L 具有性质 4. 证毕

记 A 为 L 的度量化系数,K 为 L 的度量化值,RDBMPM 将基于向量化算子 H 与度量化算子 L 来实现细粒度 RBAC 委托模型.令 $Q_x(R)$为 L 的最大取值.由定理 2 易知,$Q_x(R)=A^{n+1}-1$.

3.2 度量角色

定义 9 度量角色(R,K)

度量角色(Measuring Role)是 RDBMPM 模型通过映射算子 F 对普通角色进行扩展产生的,且只具有其唯一对应的 $E(R,\boldsymbol{\lambda})$所代表部分权限的角色,简称 M_R,其一般形式为(R,K),其中 K 称为 M_R 的度量值,$K\in N\wedge 0\leqslant K\leqslant Q_x(R)$.在 RDBMPM 中,将以度量角色来进行委托授权.所有度量角色构成角色度量集 M_{RS}.

定义 10 度量角色元组 $I(\lambda_ip_i)$

将构成(R,K)的权限集分量 λ_ip_i,$(\lambda_i>0,0\leqslant i\leqslant n)$称为 M_R 的度量元组 $I(\lambda_ip_i)$.度量角色 M_R 的所有度量元组则构成 M_R 的权限源.根据定义 8 可知,每个 M_R 都有唯一对应的权限源.令 $K_s((R,K):M_{RS})\rightarrow\lambda_jp_j$,$j\in N$,该函数将$(R,K)$映射到其唯一对应的权限源.

定义 11 度量角色关系"="和"≥"

$$(R,K)=(R',K')\Leftrightarrow R=R'\wedge K_s(R,K)=K_s(R',K')\quad(13)$$

$$(R,K)\geqslant(R',K')\Leftrightarrow\begin{cases}K_s(R,K)\supseteq K_s(R',K'),\text{if } R=R'\\(R,R')\in\mathbf{R}_H\wedge R\geqslant R',\text{if } R\neq R'\end{cases}\quad(14)$$

其中,R_H 表示普通角色之间的层次关系.如果$(R,K)\geqslant(R',K')$,一个明确授权委托(R,K)的用户可以委托(R',K').

定理 3 度量角色的(关系是偏序关系.

证明:与文[10]证明类似,易知≥关系具有自反、反对称与传递性,因而≥关系是偏序关系.

3.3 委托授权

定义 12 委托先决条件 D

先决条件 D 是用操作符"&"(与)和"|"(或)将条件角色 R_c 结合起来的布尔表达式[7].其中,R_c 的取值可为 R 或者$\bar{R}$.前者表示具有某一角色 R,后者表示不具有角色 R.

定义 13 带周期时间的时限约束 P_t

采用$([t_b,t_e],t_p)$来表示委托的有效期限和使用时间约束,$[t_b,t_e]$是一个时间段,t_p 是周期时间表达式.带周期时间约束的度量角色委托的含义是:委托用户 u_{ig}在委托操作中,仅仅赋予受托人 u_{ed}在时间段$[t_b,t_e]$以及时间周期 t_p 中执行度量角色的权力.一旦当前时间 $t>t_e$ 或不在 t_p 范围中,系统则自动撤销 u_{ed}被授予的度量角色.

定义 14 可委托授权判定

$$\boldsymbol{A}_d\subseteq R_s\times M_{RS}\times D\times P_t\times N\quad(15)$$

可委托授权关系 $\boldsymbol{A}_d$ 是一个五元组,其定义如式(15)所示.R_s,M_{RS},D,P_t,N 分别代表普通角色集、度量角色集、先决条件、周期时限约束以及最大委托次数.

当委托人 u_{ig}希望向受托人 u_{ed}进行委托时,用户先提交一个委托请求 $\boldsymbol{Z}_r=(u_{ig},u_{ed},d_r,d_c,d_p,d_n)$,系统根据 $\boldsymbol{A}_d$ 决定是否授权本次委托,如果系统判定 $\boldsymbol{Z}_r$ 是合法的,则接受该请求;反之拒绝.其中 $d_r\in M_{RS}$,$d_c\in D$,$d_p\in P_t$,$d_n\in N$.可委托授权关系 $\boldsymbol{A}_d$ 的判定过程如式(16)所示.

$$\begin{aligned}&(1)\quad u_{ig}\in\{u\mid W_u(R)\wedge(R,Q_x(R))\geqslant d_r\}\wedge\\&(2)\quad W_r(u_{ed})\in d_c\wedge\\&(3)\quad Z_r.d_p\in\Delta(Z_r).d_p\wedge\\&(4)\quad Z_r.K_s(d_r)\leqslant\Delta(Z_r).K_s(d_r')\wedge\\&(5)\quad Z_r.d_n\leqslant\Delta(Z_r).d_n\end{aligned}\quad(16)$$

其中,$W_u(R)$为角色 R 的所有用户;$W_r(u_{ed})$为受托人 u_{ed}所具备的先决条件.式(15)的具体含义为:u_{ed}满足先决条件 d_c,委托人 u_{ig}拥有 d_r 且其对 d_r 的委托能力大于本次委托中要委托给 u_{ed}的委托能力.$\Delta(Z_r)$是求本次委托 Z_r 的前驱委托请求操作,而 $\Delta(Z_r).d_p$,Δ

$(Z_r).K_s(d_r)$与 $\Delta(Z_r).d_n$ 则分别代表前驱委托的周期时限约束、度量角色的度量元组以及最大委托深度.从 A_d 的后三步可知,本次委托的使用次数、使用有效时间、最大委托深度的约束都受限于其前驱委托对三者的约束,因此,在多步委托中,委托能力是逐步收敛的,这确保了 RDBMPM 的可控性.

3.4 委托性能分析

在 $RBDM_0$ 和 RDM2000 中,委托角色 r_{ed}是以一个整体被委托出去的,即一旦将 r_{ed}委托,就必须将 r_{ed}所包含的全部权限委托出去,这种机制显然违背了"最小特权"原则.在表 1 中,给出了 RDBMPM 与这两个模型在委托性能方面[3]的对比.从表 1 可知,相比于 RDM2000、$RBDM_0$,RDBMPM 支持部分委托,因而能很好地满足用户在细致委托方面的需求,且因度量角色具有层次结构(定理 3)及支持委托次数、周期性时间约束等临时性方面的限制,从而增强了模型的可管理性与可控性.

表 1　RDBMPM 与 RDM2000、$RBDM_0$ 的委托性能对比

性质 / 模型	委托粒度		委托层次	委托传播		临时性限制	
	total	Partial	hierarchy	single-step	multi-step	times	periodicity
RDBMPM	O	O	O	O	O	O	O
RDM2000	O	×	×	O	O	×	×
$RBDM_0$	O	×	×	O	×	×	×

3.5 模型的应用

RDBMPM 提出从角色委托需求集到自然数集的映射机制来解决细粒度角色委托问题,相对于现有三个支持部分委托的模型:$PBDM_0$、QBCDM 与 RPRDM,RDBMPM 的抽象化程度将更高.下面通过不同的映射过程,给出如何基于 RDBMPM 来得到这三个典型模型的实现.

3.5.1 $PBDM_0$ 的实现

$PBDM_0$[6]通过创建临时角色 T_R,并为之分配期望的权限来实现部分委托.临时角色与度量角色在委托模型中的作用是类似的,它们都代表用户-用户的部分委托.但在 RDBMPM 中,系统预先将所有部分委托权限的组合通过映射算子 F 作用后得到度量角色集,并将映射关系保存下来.当一个用户向其他用户进行委托时,用户将只需提交请求 (R,K),系统再按照逆算子 F^{-1}就可找到委托人所期望委托的权限.下面给出利用度量角色来实现临时角色的功能,如式(17)所示.

$$\begin{aligned}&(1)H(E(R,\lambda)=\boldsymbol{x},\boldsymbol{\lambda}=(\lambda_0,\lambda_1,\cdots,\lambda_n),\text{且 }\lambda_i\in\{0,1\};\\&(2)L(\boldsymbol{x})=L(x_0,x_1,\cdots,x_n)=K;\\&(3)T_R=(R,K)\end{aligned}\tag{17}$$

3.5.2 RPRDM 的实现

RPRDM[9]的基本思想为:令委托角色 $r_{ed}=\{p_1,p_2,\cdots,p_n\}$,$p_i(1\leqslant i\leqslant n)$是 r_{ed}所具有的权限项,$T_{\text{mask}}=(b_1,b_2,\cdots,b_n)$,$b_i$ 是 T_{mask}的二进制数位,$b_i\in\{0,1\}$.当 $b_i=1$,表示本次委托包含 p_i,反之当 $b_i=0$ 时,本次委托将不包含 p_i.RPRDM 的屏蔽值 T_{mask}机制可通过映射机制 F 的向量化算子 H 来实现,其本质上是实现从任意一个部分角色授权需求到一组二进制数位的映射.下面给出基于 RDBMPM 来实现 RPRDM,整个过程如式(18)所示.

$$\begin{aligned}&(1)E(R,\boldsymbol{\lambda})=\boldsymbol{\lambda}\boldsymbol{p}^{\mathrm{T}},\lambda=(\lambda_0,\lambda_1,\cdots,\lambda_n),\\&\quad\boldsymbol{p}=(p_0,p_1,\cdots,p_n),\text{且 }\lambda_i\in\{0,1\};\\&(2)\boldsymbol{V}(R,\boldsymbol{\lambda})=\mathrm{Vector}(E(R,\boldsymbol{\lambda}))=\boldsymbol{\lambda};\\&(3)\boldsymbol{G}=\mathrm{diag}(\boldsymbol{g}_0^{\mathrm{T}},\boldsymbol{g}_1^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}});\\&(4)\boldsymbol{x}=(x_0,x_1,\cdots,x_n)=J(\boldsymbol{V}(R,\boldsymbol{\lambda}))=\boldsymbol{\lambda}\cdot\boldsymbol{G}^{-1};\\&(5)T_{\text{mask}}=\boldsymbol{x}.\end{aligned}\tag{18}$$

3.5.3 QBCDM 的实现

QBCDM 中采用量化角色 Q_R 来支持细粒度角色授权[10].虽然量化角色 Q_R 与度量角色 M_R 都可认为是从任意一个部分角色授权需求到一个唯一标识符 (R,K) 的映射,但因度量角色是基于 $E(R,\boldsymbol{\lambda})$出发得到的,即其本身考虑了因权限重要性而引起的同一委托中使用次数限制的不同,从而更能满足实际的需要.同样,量化角色可以通过特殊化映射机制 F 中的向量化算子 H 和度量化算子 S 来产生,式(19)给出了 QBCDM 在 RDBMPM 中的实现过程.

$$\begin{aligned}&(1)E(R,\boldsymbol{\lambda})=\boldsymbol{\lambda}\boldsymbol{p}^{\mathrm{T}},\lambda_i\in\{0,1\},i=0,1,\cdots,n;\\&(2)\boldsymbol{V}(R,\boldsymbol{\lambda})=\mathrm{Vector}(\boldsymbol{\lambda}\boldsymbol{p}^{\mathrm{T}})=\boldsymbol{\lambda}=(\lambda_0,\lambda_1,\cdots,\lambda_n);\\&(3)\boldsymbol{x}=\boldsymbol{V}(R,\lambda)\cdot\boldsymbol{G}^{-1}=\boldsymbol{\lambda}\cdot\boldsymbol{G}^{-1},\boldsymbol{G}=\mathrm{diag}(\boldsymbol{g}_0^{\mathrm{T}},\boldsymbol{g}_1^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}});\\&(4)\text{取 }S=L,\text{其中 }L\text{ 的度量化系数}A=2;\\&(5)K=L(x_0,x_1,\cdots,x_n);\\&(6)Q_R=(R,K).\end{aligned}\tag{19}$$

4 结论

针对现有 RBAC 委托模型在细致委托方面存在的不足,本文通过分析细粒度 RBAC 授权许可之间的关系,提出一种基于映射机制的细粒度 RBAC 委托授权模型 RDBMPM,该模型基于向量化与度量化算子的复合运算提出了度量角色的概念.为增加在委托过程中的可控性,本文也对模型的约束机制进行了相关研究,保证了模型在权限传播中的收敛性.最后,通过给出三个典型的支持细粒度委托的模型在 RDBMPM 中的实现,进而验证了基于映射机制的角色委托模型的理论研究价值.

根据委托应用的需要,本文抽象地构造出了 RBAC 度量化算子的整体性质,并给出一类满足其定义的构造方法,对于其他构造方法的研究将是本文的下一步工作.此外,RDBMPM 在具体应用方面的研究也是我们未来的工作重点.

参考文献:

[1] Mavridis I, Mattas A, Pagkalos I, et al. Supporting dynamic administration of RBAC in web-based collaborative applications during run-time[J]. International Journal of Information and Computer Security, 2008, 2(4): 328 – 352.

[2] 郑吉平,秦小麟,等.基于数字水印的数据库角色访问控制模型[J].电子学报,2006,34(10):1906 – 1910.
Zheng Ji-ping, Qin Xiao-lin, et al. Digital watermark based database model using RBAC[J]. Acta Electronica Sinica, 2006, 34(10): 1906 – 1910. (in Chinese)

[3] Barka E, Sandhu R. Framework for role-based delegation models[A]. Werner B. Proceedings of the 16th Annual Computer Security Applications Conference[C]. New Orleans: IEEE Computer Society, 2000. 168 – 176.

[4] Barka E, Sandhu R. A role-based delegation model and some extensions[A]. Mehuron W. Proceedings of the 23rd National Information Systems Security Conference[C]. Maryland: NIST, 2000. 101 – 114.

[5] Barka E, Sandhu R. Role-based delegation model/hierarchical roles (RBDM1)[A]. Thomsen D. Proceedings of the 20th Annual Computer Security Applications Conference[C]. Washington DC: IEEE Computer Society, 2004. 396 – 404.

[6] Zhang L, Ahn G J, Chu B T. A rule-based framework for role-based delegation and revocation[J]. ACM Transactions on Information and System Security, 2003, 6(3): 404 – 441.

[7] Zhang X W, OH S, Sandhu R S. PBDM: A flexible delegation model in RBAC[A]. Ferrari E. Proceedings of the 8th ACM Symposium on Access Control Models and Technologies[C]. New York: ACM Press, 2003. 149 – 157.

[8] Wainer J, Kumar A. A fine-grained, controllable user-to-user delegation method in RBAC[A]. Ferrari E. Proceedings of the 10th ACM Symposium on Access Control Models and Technologies[C]. New York: ACM Press, 2005. 59 – 66.

[9] Cramption J, Khambhammettu H. Delegation in role-based access control[J]. International Journal of Information Security, 2008, 7(2): 123 – 136.

[10] 赵庆松,孙玉芳,孙波.RPRDM:基于重复和部分角色的转授权模型[J].计算机研究与发展,2003,40(2):221 – 227.
Zhao Qing-song, Sun Yu-fang, Sun Bo. RPRDM: A repeated-and-art-role-based delegation model[J]. Journal of Computer Research and Development, 2003, 40(2): 221 – 227. (in Chinese)

[11] 翟征德.基于量化角色的可控委托模型[J].计算机学报,2006,29(8):1401 – 1407.
Zhai Zheng-de. Quantified-role based controlled delegation model[J]. Chinese Journal of Computer, 2006, 29(8): 1401 – 1407. (in Chinese)

作者简介:

蔡伟鸿 男,1963 年出生于广东潮州,华南理工大学博士生、汕头大学计算机系教授,主要研究方向为网络与通信、信息安全研究与应用.
E-mail: whcai@stu.edu.cn

韦 岗 男,1963 年出生于广西宾阳,华南理工大学电子与信息学院博士生导师,主要研究方向为通信、信息处理理论与技术.
E-mail: ecgwei@scut.edu.cn