Journal of Computer Applications
计算机应用,2013,33(8):2218 - 2221
ISSN 1001-9081
CODEN JYIIDU
2013-08-01
http://www.joca.cn

文章编号:1001-9081(2013)08-2218-04
doi:10.11772/j.issn.1001-9081.2013.08.2218

移动环境多角色安全互斥风险的模糊评估

王建军[1,2*],李建平[1]
(1.电子科技大学 计算机科学与工程学院,成都 610054; 2.湖南第一师范学院 信息科学与工程系,长沙 410002)
(*通信作者电子邮箱 wjj5351@163.com)

摘 要:传统机制解决移动环境多角色安全互斥问题的效率较低,为此,提出利用多角色综合敏感度评判安全互斥程度的解决方案。系统基于角色内部安全因素模糊评判角色敏感度,再采用补偿竞争算法计算多角色综合敏感度,即对角色敏感度进行海明距离补偿,取补偿后的最大值为多角色综合敏感度,使移动环境多角色系统在安全和效率间取得平衡。最后,分析了算法的复杂度,使用实例论证了算法可以提高角色的执行效率。

关键词:移动计算;安全互斥;模糊评判;敏感度;风险值
中图分类号:TP393.07 **文献标志码**:A

Fuzzy risk evaluation on multi-role security mutual exclusion in mobile environment

WANG Jianjun[1,2*], LI Jianping[1]
(1. *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*; 2. *Department of Information Science and Technology, Hunan First Normal University, Changsha Hunan* 410002, *China*)

Abstract: Since the traditional mechanism is low in efficiency to solve the multi-role security mutex in the mobile environment, a solution was proposed to determine the degree of security mutex using the multi-role comprehensive sensitivity. The system carried out fuzzy evaluation on the sensitivity of a role based on the internal security factors of the role, then calculated the comprehensive sensitivity of multiple roles utilizing the compensation competitive algorithm, i.e. did the Hamming distance compensation to the role sensitivity, took the compensated maximum as the multi-role comprehensive sensitivity, enabling the multi-role system in the mobile environment to achieve a balance between safety and efficiency. Finally, the algorithm has been analyzed for its complexity and an example demonstrates that the algorithm can increase the execution efficiency of the roles.

Key words: mobile computing; security mutual exclusion; fuzzy evaluation; sensitivity; value-at-risk

《计算机应用》Journal of Computer Applications

0 引言

基于角色访问控制(Role-Based Access Cotrol,RBAC)[1]是移动环境(如 Ad Hoc)的主要安全策略,角色权限受时态约束,在同时态区间一个角色可能继承或执行多个互斥角色,或多个互斥角色可能动态构成一个交互系统。传统 RBAC 采取任务分离机制解决互斥问题;通用时态约束基于角色访问控制(Generalized Temporal Role-Based Access Cotrol,GTRBAC)[2]使用强方式和弱方式,强方式中互斥角色完全独立,不利于角色权限灵活变更,弱方式中互斥角色完全包容,不利于角色安全;“中国墙”[3]策略直接将利益冲突双方相互隔离。不管是传统 RBAC、GTRBAC,还是“中国墙”,角色互斥关系都是静态的,是“两两”互斥,在判断移动环境多角色互斥关系时具有局限性。虽然 RBAC 可以对多角色分组,仅使同组角色具有相同权限,但不能决定角色之间的互斥关系。

按照互斥产生的原因,角色互斥可以分为时序互斥、内容互斥和安全互斥。时序互斥指角色具有先后执行时序;内容互斥指角色内容不允许同时执行;时序互斥和内容互斥是显性互斥关系,可以通过改变角色的执行时序解决。安全互斥指角色执行时存在信息安全风险,如石油公司 A 的客户信息和石油公司 B 的客户信息存在安全互斥风险。安全互斥需要考虑互斥程度,如石油公司 A 和 B 以及电信公司 C,因为 A 和 B 存在利益冲突,A 和 B 的客户信息安全互斥程度应该大于 A 和 C 或者 B 和 C。本文仅涉及安全互斥。

模糊信任和风险评估是分布式 RBAC 应用的主要安全措施。文献[4]指出安全具有模糊性,使用模糊逻辑描述多级安全策略。信任度或敏感度是实现角色任务模糊分离的主要机制。文献[5 - 7]中信任度或敏感度是静态的,文献[8 - 10]借用上下文环境使信任度具有动态性。模糊信任是基于上下文环境、用户属性等信息,使用模糊方法计算用户的信任度,并根据信任度或敏感度决定是否给用户授权。因为上下文环境和用户属性等信息的收集有一定局限性,基于信任授权并不能完全防范安全风险,尤其是合法用户的非法行为,如角色误用和滥用等。风险评估对用户访问进行风险分析并给出安全评价。文献[11 - 12]针对用户信任、访问行为和角色历史等信息对用户访问请求进行风险评估,建立风险自适应的分布式数据库系统 RBAC;文献[13]基于 RT^R 实现带风险约束的分布式环境角色授权和委托授权模型,由边风险聚合为路径风险;文献[14]按风险大小将风险图中的角色划分到不同的风险带中,定义了带风险约束的许可分配规则;文献

收稿日期:2013-03-11;**修回日期**:2013-05-06。
基金项目:湖南省高校科技创新团队支持计划项目(湘教通[2010]212 号);湖南省教育厅科技计划项目(10C0528)。
作者简介:王建军(1969 -),男,湖南衡阳人,副教授,博士研究生,主要研究方向:网络信息安全; 李建平(1965 -),男,湖南祁阳人,教授,博士生导师,博士,主要研究方向:网络信息安全。

[15]定义了模糊多级安全(Multi_Level Security,MLS),使用 Sigmoid 函数建立敏感度与信息泄漏风险的关系;文献[16]实现了模糊风险 BLP,定义了多风险因素的连接、析取、包含和聚合等操作规则及风险访问控制系统,文献[17]则实现了文献[16]的风险访问控制原型;文献[18]能够对用户的角色需求进行风险预估,通过调整风险门限值既满足用户合适的角色需求,又防止滥用角色权限;文献[19]建立了基于随时间推移的风险值预估信任模型,限制恶意节点的行为。风险技术有两个明显的趋势,一是求角色集合风险值,二是对角色风险进行预估。角色风险值由系统根据上下文环境和用户行为判定,角色集合风险值则是相关角色风险值的和值;风险预估可以控制用户的行为。用户行为易具有欺骗性,判断用户行为特征有一定难度;敏感度给用户、角色和客体三者之间的安全提供被动保护;上下文环境、用户属性和用户行为是角色安全的外因,移动环境角色之间关系随机变化,仅由外因考虑角色安全不太客观,角色安全内部因素是角色安全脆弱性的根本原因,因此角色安全可以通过优化角色内部机制而改进;对于分布式多角色环境,需要考虑角色之间的安全关系,尤其是安全互斥,虽然不同角色之间可以依靠信任链传递信任,但中间环节可能影响可靠性,另外角色集合的风险值与角色的风险值不是线性关系,不能简单地通过求和实现。

本文从角色内部因素判断角色敏感度,即对因为角色内部安全缺陷可能引起的角色信息随机泄漏、角色信息误读和角色信息误写三个方面的脆弱性进行模糊综合评判,敏感度指角色的信息安全强度。对于角色集合,即多个角色同时被继承或执行,或多个角色构成一个交互系统,信息安全强度表示为多角色综合敏感度,与相关角色的敏感度有关。多角色综合敏感度计算引入文献[16]角色结合时风险值计算基本思想,综合敏感度不是相关角色敏感度的累加或平均,而是通过相关角色敏感度的补偿竞争获得。风险值表示继承或执行角色时发生信息安全事故的概率,受敏感度影响。本文讨论多角色间安全互斥关系的模糊评判策略。

1　多角色互斥关系的模糊评判

为方便阅读,本文使用的所有变量如表 1 所示。

表 1　变量介绍

变量名	说明	变量名	说明	变量名	说明
Sen	敏感度	w	斜率	U	敏感度因素
Sen'	综合敏感度	k	第 i 个因素获得评价的总人数	V	敏感度等级
VaR	风险值	A	权值	C_{ij}	第 i 个因素获得第 j 等级评价的人数
Sen_{star}	敏感度区间始值	$\boldsymbol{S}$	单因素评判矩阵	p	滑动窗口大小,$p \in \mathbf{N}$ 且 $p > 1$
Sen_{end}	敏感度区间终值	$\boldsymbol{B'}$	综合评判矩阵	q	$q \in \mathbf{N}$ 且 $1 \leqslant q \leqslant (p-1)$
VaR_{thr}	风险值门限	P	角色许可	m	数组大小
Sen_{thr}	敏感度门限	T	角色时态		

1.1　敏感度和风险值

风险值和敏感度关系具有三个特性:

1)风险值是敏感度的正函数;

2)风险值变化速率是敏感度变化速率的正函数;

3)风险值具有阶跃性。

如果 $Sen \in \mathbf{N}, 0 < VaR < 1$,由敏感度和风险值关系特性可知,$VaR$ 和 Sen 之间的关系可由 Sigmoid 函数表示,VaR_{thr} 为阶跃点,式(1)为 VaR 关于 Sen 的 Sigmoid 函数表达式。

$$VaR = \frac{1}{1 + \exp(-Sen)} \tag{1}$$

按照概率密度函数正态分布规律,Sen 应主要位于区间 $[Sen_{star}, Sen_{end}]$ 中心点附近,Sen_{thr} 对应 VaR_{thr},二者可动态调整且不一定同步,改进式(1)为式(2),可使 VaR_{thr} 和 Sen_{thr} 交于 Sigmoid 函数曲线的中心,0.5 为式(1)中心点的 VaR 值。

$$VaR - (0.5 - VaR_{thr}) = \frac{1}{1 + \exp(-w(Sen - Sen_{thr}))} \tag{2}$$

1.2　角色敏感度

模糊综合评判的对象为每个角色的角色信息随机泄漏、角色信息误读和角色信息误写三个因素,每个角色均有一个功能描述表针对三个因素进行描述,作为角色相互评价的依据,角色评价者可以由项目组成员或角色拥有者担当。

角色敏感度的因素 $U = \{u_1, u_2, u_3\}$,u_1 表示角色间信息随机泄漏,u_2 表示角色间信息误读,u_3 表示角色间信息误写。与敏感度等级相对应的评判集 $V = \{v_1, v_2, \cdots, v_n\}$ 表示安全等级,如果 $V = \{v_1, v_2, v_3, v_4, v_5\}$,其中 v_1 为低,v_2 为较低,v_3 为中,v_4 为较高,v_5 为高,对应 Sen 分别为(5,4,3,2,1)。有 n 个角色评价者根据角色描述对每个角色三个因素作出风险评价,C_{ij} 表示第 i 个因素获得第 j 安全等级评价的人数,其中 $\sum_{j=1}^{5} c_{ij} = k_i (k_i \leqslant n, i \in \{1,2,3\}, j \in \{1,2,3,4,5\})$。

令 $r_{ij} = c_{ij}/k_i$,得单因素评判矩阵如式(3):

$$\boldsymbol{S} = \begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ r_{31} & r_{32} & r_{33} & r_{34} & r_{35} \end{bmatrix} \tag{3}$$

内部因素权值 $A = (a_1, a_2, a_3)$,$\sum_{i=1}^{3} a_i = 1, a_i > 0$ 且可动态调整。使用模型 $M(\wedge, \vee)$ 计算,得综合评判结果如式(4)所示:

$$\boldsymbol{B'} = A \circ \boldsymbol{S} = (b_1, b_2, b_3, b_4, b_5) \tag{4}$$

将 $\{b_1, b_2, b_3, b_4, b_5\}$ 匹配 $\{v_1, v_2, v_3, v_4, v_5\}$,按最大隶属度原则,取 $\vee \{b_1, b_2, b_3, b_4, b_5\}$ 所对应的 v_i 为角色的敏感度。

1.3　多角色综合敏感度

按照文献[16]规则“两个风险值低的角色相结合后,综合风险值低”,这也符合人类社会的一般规则,如“两个脾气好的人相互生气概率低”,本文多角色综合敏感度计算思想以此为基础并改进。

多角色综合敏感度是对多角色共存安全互斥情况的基本判断,不考虑异常情况。据此分析,m 个角色的综合敏感度应该接近相关角色敏感度平均值,但直接使用平均值作为综合敏感度不太合适,因为综合敏感度应该考虑敏感度门限值,也应尽可能贴近敏感度门限值。这样有两点好处,一是如果

《计算机应用》Journal of Computer Applications

$Sen' < Sen_{thr}$,则选取$[Sen_{star}, Sen_{thr})$中最大值为Sen',可使更多的角色能够继承或执行;二是如果$Sen' \geqslant Sen_{thr}$,则选取$[Sen_{thr}, Sen_{end}]$中最小值为Sen',可使更少的角色不被继承或执行。

1.3.1 算法规则

规则1 Sen'绝对值应尽可能最低,以尽可能使角色群能够继承或执行更多的角色。

规则2 Sen'相对值应尽可能最大,以尽可能保障角色间信息安全。

规则3 $Sen' \in [Sen_{star}, Sen_{end}]$,$Sen'$值在区间的分布符合概率密度函数正态分布,使$Sen'$尽可能贴近$Sen_{thr}$。

1.3.2 算法描述

算法采取补偿竞争方法,先使用角色敏感度与Sen_{thr}之间海明距离的平均值α按比例差对各角色敏感度进行补偿,再取补偿后角色敏感度中的最大值为Sen'。根据规则3,以海明距离联系各角色敏感度,通过式(2)调整,可以使Sen_{thr}位于曲线的中心,以Sen_{thr}为基值,计算各角色敏感度与Sen_{thr}之间的海明距离及其平均值α。根据规则1,应该调整相关角色敏感度,使之趋向平衡,以便Sen'贴近Sen_{thr},使更多的角色能够继承或执行。考虑不同角色群的特征,以该角色群敏感度平均值而非敏感度区间中心值为中值,小于中值的敏感度按比例差加上修正值α,大于中值的敏感度按比例差减去修正值α。根据规则2,比较修正后的敏感度,取最大值为Sen',因Sen_{thr}和VaR_{thr}值非同步变化,需比较VaR和VaR_{thr}。

2 算法实现

因为增加了敏感度约束,将时态约束角色R的数据结构(P,T)扩展为(P,T,Sen)。如果某时态区间有m个角色,以继承节点R_0为根节点,角色按敏感度由小到大排序构成m叉树,如图1所示。

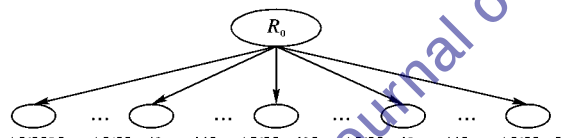

图1 m叉树

2.1 两角色综合敏感度计算

如果$m = 2$,用户执行角色$R_1(P_1,T,Sen(1))$和$R_2(P_2,T,Sen(2))$,过程1为求两角色综合敏感度。

过程1 两角色综合敏感度计算。

步骤1 $\alpha = (|Sen_{thr} - Sen(1)| + |Sen_{thr} - Sen(2)|)/2$;

步骤2 如果$Sen(1) \leqslant Sen(2)$,则$Sen' = \vee \{Sen(1) + \alpha, Sen(2) - \alpha\}$,否则$Sen' = \vee \{Sen(2) + \alpha, Sen(1) - \alpha\}$。

2.2 多角色综合敏感度计算

多角色综合敏感度算法使用滑动窗口,窗口大小为p,即一次最多允许继承执行的角色数,需要继承执行的角色进入窗口,窗口内角色综合敏感度的门限值为Sen_{thr}。对于m个角色,分别为$R_1(P_1, T, Sen(1))$, $R_2(P_2, T, Sen(2))$, …, $R_m(P_m, T, Sen(m))$。

过程2 多角色综合敏感度计算。

步骤1 如果$m \leqslant p$,则m个角色全部进入窗口;如果$m > p$,将m划分成$(p-1)$个区间,分别取R序号值为$(1, \lceil m/(p-1) \rceil, 2\lceil m/(p-1) \rceil, \cdots, q\lceil m/(p-1) \rceil, \cdots, m)$的角色敏感度进入窗口,使每轮次进入窗口的角色敏感度基本均衡;如果$q\lceil m/(p-1) \rceil \geqslant m$,则$R$序号值取$m$。

步骤2 $\alpha = \sum_{i=1}^{m} |Sen_{thr} - Sen(i)| / m$。

步骤3 $Sen' = \vee (Sen(1) + \alpha, Sen(\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil, Sen(2\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil (1 - (2/p)), \cdots, Sen(\lceil m/2 \rceil), \cdots, Sen(q\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil (1 - (2q/p)), \cdots, Sen((p-2)\lceil m/(p-1) \rceil) + (\lceil 2\alpha/(p-1) \rceil (-1 + (2/p)) + (-\alpha)), Sen(m) + (-\alpha))$。

步骤4 将Sen'代入式(2)中的Sen,计算VaR。

步骤5 如果$VaR < VaR_{thr}$,则继承执行窗口中的角色;如果$VaR \geqslant VaR_{thr}$,则$Sen' = \vee (Sen(1) + \alpha, Sen(\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil, Sen(2\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil (1 - (2/p)), \cdots, Sen(\lceil m/2 \rceil), \cdots, Sen(q\lceil m/(p-1) \rceil) + \lceil 2\alpha/p \rceil (1 - (2q/p)), \cdots, Sen((p-2)\lceil m/(p-1) \rceil) + (\lceil 2\alpha/(p-1) \rceil (-1 + (2/p)) + (-\alpha)))$;窗口回退第$m$个角色,回退角色单独继承执行;依此类推,至窗口中所有角色执行完毕。

步骤6 删除已继承或执行角色,构建新的角色序列$(R_1(P_1,T,Sen(1)), R_2(P_2, T, Sen(2)), \cdots, R_{m-p}(P_{m-p}, T, Sen(m-p)))$;

步骤7 循环执行步骤1 ~ 6,直至m个角色继承执行。

3 算法分析和论证

3.1 算法分析

如果角色执行时间为t,n个角色连续执行时间为nt,遍历时间为n,时间复杂度为$(nt + n)$。使用滑动窗口,排序的时间复杂度为$O(nm)$,假定窗口大小为p,最理想情况,每轮次窗口中p个角色均可以继承,时间复杂度为$O(nt/p)$;遍历兼初始化所需时间为n,算法的时间复杂度为$O(nt/p + n + nm)$;如果t较大,滑动窗口能显著提高系统运行效率,特别对于敏感度全小于Sen_{thr}的多角色;最糟糕情况是每个角色单独执行,算法的时间复杂度为$O(nt + n + n(p+1)/2 + nm)$,如果$n$值太大,滑动窗口会比较明显地降低系统运行效率,在敏感度全大于Sen_{thr}时可能存在。按照概率分布规律,最理想情况和最糟糕情况出现的机会极低,如果窗口每轮次平均回退1个角色,则算法的时间复杂度为$O(nt/p + n + nm + n(2p-1)/p)$,对系统效率影响需要比较$t$和$n$。一般情况下系统运行时间主要由角色的执行时间$t$决定,算法明显优化了系统运行效率,但每轮次窗口平均回退角色增加,则系统运行时间仍会增加,故角色的优化组合规则非常重要。

3.2 实例论证

移动网络(如Ad Hoc)中一个移动角色请求访问其他11个资源角色,需判断11个资源角色的安全互斥关系。11个资源角色的管理者相互给出角色评价,且模糊评判计算出每个角色的敏感度,资源角色序列为$(B_1,B_2,B_3,B_4,B_5,B_6,B_7,B_8,B_9,B_{10},B_{11})$,对应的敏感度分别为(1,1,1,2,2,3,3,3,4,4,5),窗口大小为5,风险值门限为0.5,$Sen_{thr} = 3$。

根据算法,第1轮取角色(B_1,B_3,B_6,B_9,B_{11}),对应的敏感度为(1,1,3,4,5),海明距离均值为1.4,经补偿计算得角色综合敏感度$Sen = 3.6 > 3$,滑动窗口回退1个角色,窗口内角色敏感度序列为(1,1,3,4),经补偿计算得角色综合敏感度$Sen = 2.75 < 3$,代入式(2),得$VaR = \frac{1}{1 + e^{-(2.75-3)}} < 0.5$,

《计算机应用》Journal of Computer Applications

故角色序列(B_1,B_3,B_6,B_9)可继承执行;角色B_{11}则需单独继承执行。

第二轮取剩下角色序列(B_2,B_4,B_5,B_7,B_8,B_{10})中的角色(B_2,B_5,B_7,B_8,B_{10})进入滑动窗口,对应敏感度值分别为(1,2,3,3,4),计算可得修正敏感度为0.8,综合敏感度$Sen = 3.2 > 3$,滑动窗口需回退1个角色,窗口内剩下角色敏感度为(1,2,3,3),计算可得修正敏感度为0.75,角色综合敏感度$Sen = 2.625 < 3$,代入式(2),得$VaR = \frac{1}{1 + e^{-(2.625-3)}} < 0.5$,故角色序列($B_2$,$B_5$,$B_7$,$B_8$)可合并执行;角色$B_{10}$则需单独继承执行。

最后一轮仅剩下角色B_9,单独继承执行。

从经验也可得出,敏感度低的角色继承执行风险较低,第一、二轮分别回退1个敏感度最高的角色,再继承执行剩下的角色,可以明显降低继承执行风险,与以上计算判断结果基本一致。

4　结语

本文将传统的、由外部因素判定的互斥关系改变由角色的内部因素判定,克服了移动计算中用户与角色、角色与角色之间关系的随机性和动态性所带来的影响,给多角色系统安全和效率提供了一个综合平衡的解决方案。针对多角色环境提出的模糊改进方案具有以下特点与优势:

1)算法可以用于移动计算、云计算和协同计算等陌生角色交互访问的安全互斥判断,不需要依赖行为特征和访问历史。

2)多角色合并继承执行有利于提高角色序列执行的效率,在按照流程处理的业务中,其需求较多,例如审计业务、会计核算业务、移动节点按时序访问资源等。

3)模糊综合评判方案存在两个动态决策点,即风险评判和风险因素权值设定具有动态性,可以动态改变角色的敏感度并影响角色的权限继承和执行序列,提高角色执行的灵活性。例如医院院长具有管理者和医生两个角色且互斥,在紧急情况下需要在管理者时态区间执行医生角色,可以通过改变敏感度降低互斥度,使两个角色能够合并继承执行。

4)针对多个角色合并继承执行提出的安全模糊评判方案,可以有效提高角色执行的综合安全性。例如作为律师,他可以选择给A公司当法律顾问,也可以选择给B公司当法律顾问,如果同时执行,可能存在信息泄漏风险,A公司可以通过改进自身的安全因素,避免信息泄漏。

5)增加敏感度约束的角色对RBAC的其他机制没有制约,因为其他机制不会涉及角色间互斥问题,不会因为增加角色敏感度约束而增加其机制的复杂性。

本文提供的是多角色安全互斥的基本评判方法,如果对安全有特别要求,需要对角色间的安全机制进一步细化;扎德算子可能遗漏角色信息,也需要改进。这些都是本文的后续工作。

参考文献:

[1] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38 – 47.

[2] JOSHI J B D, BERTINO E, LATIF U, *et al*. A generalized temporal role-based access control model [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(1): 4 – 23.

[3] BREWER D F C, NASH M. The Chinese wall security policy [C]// Proceedings of the 1989 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 1989: 206 – 214.

[4] HOSMER H H. Using fuzzy logic to represent security policies in the multipolicy paradigm [J]. ACM SIGSAC Reviews, 1992, 10(4): 12 – 21.

[5] TAKABI H, AMINI M. Separation of duty in role-based access control model through fuzzy relation[C]// IAS 2007: Proceedings of the Third International Symposium on Information Assurance and Security. Piscataway: IEEE, 2007: 125 – 130.

[6] NAWARATHNA U H G R D, KODITHUWAKKU S R. A fuzzy role based access control model for database security[C]// Proceedings of the 2005 International Conference on Information and Automation. Piscataway: IEEE, 2005: 313 – 318.

[7] MARTINEZ-GARCÍA C, NAVARRO-ARRIBAS G, BORRELL J. Fuzzy role-based access control[J]. Information Processing Letters, 2011, 111(10): 483 – 487.

[8] 窦文阳, 王小明, 张立臣. 普适环境下的动态模糊访问控制模型研究[J]. 计算机科学, 2010, 37(9): 63 – 67.

[9] 刘武, 段海新, 张洪, 等. TRBAC: 基于信任的访问控制模型[J]. 计算机研究与发展, 2011, 48(8): 1414 – 1420.

[10] 王艳辉, 肖雪梅, 贾利民. 互操作信任的模糊变权动态综合评价方法[J]. 计算机研究与发展, 2012, 49(6): 1235 – 1242.

[11] CELIKEL E, KANTARCIOGLU M, THURAISINGHAN B, *et al*. Managing risks in RBAC employed distributed environments [C]// On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, LNCS 4804. Berlin: Springer, 2007: 1548 – 1566.

[12] CELIKEL E, KANTARCIOGLU M, THURAIINGHAM B M, *et al*. A risk management approach to RBAC[J]. Risk and Decision Analysis, 2009, 1(2): 21 – 33.

[13] CHAPIN P, SKALKA C, WANG X S. Risk assessment in distributed authorization[C]// FMSE'05: Proceedings of the 2005 ACM Workshop on Formal methods in Security Engineering. New York: ACM, 2005: 33 – 42.

[14] NISSANKE N, KHAYAT E J. Risk based security analysis of permissions in RBAC[C]// ICEIS 2004: Proceedings of the 2nd International Workshop on Security in Information Systems, Security in Information Systems. Porto, Portugal: INSTICC Press, 2004: 332 – 341.

[15] CHENG P C, ROHATGI P, WAGNER G M, *et al*. Fuzzy multilevel security: an experiment on quantified risk-adaptive access control[C]// SP'07: Proceedings of the 2007IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2007: 222 – 230.

[16] NI Q, BERTINO E, LOBO J. Risk-based access control systems built on fuzzy inferences[C]// ASIACCS'10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2010: 250 – 260.

[17] CHARI S, LOBO J, MOLLOY I. Practical risk aggregation in RBAC models[C]// SACMAT'12: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies. New York: ACM, 2012: 117 – 118.

[18] BARACALDO N, JOSHI J. A trust-and-risk aware RBAC framework: tackling insider threat[C]// SACMAT'12: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies. New York: ACM, 2012: 167 – 176.

[19] 郭一凡, 李腾, 郭玉翠. P2P 网络中基于随时间推移的风险值评估的信任管理模型[J]. 计算机应用, 2012, 32(9): 2613 – 2616.

《计算机应用》Journal of Computer Applications