FSP:一种基于风险的安全策略

杨 勇,孙宇清,周 丽
YANG Yong,SUN Yu-qing,ZHOU Li

山东大学 计算机科学与技术学院,济南 250101
Department of Computer Science and Technology,Shandong University,Jinan 250101,China
E-mail:hello_yy@sina.com.cn

YANG Yong,SUN Yu-qing,ZHOU Li.FSP:Risk-based security policy.Computer Engineering and Applications,2010,46(13):82-86.

Abstract: Separation of duty is an extremely important and widely used security policy,which requires a sensitive task to be performed by a team of at least k users.However,current literatures do not capture the requirements of detailed qualification analysis on users involved in the task.Here,Role Based Access Control(RBAC) systems are focused on,and a novel risk-based Fuzzy Security Policy(FSP) is introduced based on the authorization risk resulted by user-role assignments.The risk-level vector is adopted to quantify such risk and the method of calculating the risk aggregation for multiple users performing multiple tasks is also presented.By using fuzzy comprehensive evaluation method,the FSP satisfiability problem under a given system configuration and an acceptable risk threshold is discussed.The corresponding algorithm is presented as well.This security policy will help to select suitable users to perform the task for an organization.

Key words: access control;security policy;risk

摘 要:针对基于角色的访问控制模型(RBAC)和职责分离(SoD)这一重要的安全原则,提出了一种基于风险的安全策略—Fuzzy Security Policy(FSP),采用资质表达式限定执行敏感任务的用户数量和身份,采用风险度向量方法量化用户角色授权风险,运用模糊综合评估法分析满足资质约束的用户集执行多项任务的聚集风险;进一步讨论了给定系统配置和风险阈值的安全策略的可满足性,并给出了判定用户集是否满足安全策略的算法。这种安全策略可以为组织选择符合安全需求的用户集执行任务。

关键词:访问控制;安全策略;风险
DOI:10.3778/j.issn.1002-8331.2010.13.025 **文章编号:**1002-8331(2010)13-0082-05 **文献标识码:**A **中图分类号:**TP309

1 引言

访问控制是保证信息系统安全的基本措施,它决定了谁有权使用以及如何使用系统的资源。职责分离(SoD)是访问控制中最广泛使用的安全策略,其基本定义是"将敏感信息中的职责进行分割,以避免使个人的行为危及到整个数据处理系统的安全",其基本形式是限定了敏感任务至少由一定数量的用户一起完成[1]。Nash 等人[2]解释了静态和动态职责分离的执行区别,此后,许多基于 RBAC 模型[3]的约束被提出[4-6],它们或者是新的约束分类或者是新的约束语言,用于实现不同的角色互斥约束。Li 等人提出的安全策略代数方法[7]扩充了职责分离约束的表达能力,可以限定用户身份,如一个财务工作要求执行用户中有一名拥有注册会计师资格的会计。但是,上述方法只是定性地分析了这种约束的可满足性,难以满足敏感任务的更细致的安全需求,如当多个用户集满足约束且需要选择最优的用户集时,由于不能够分析评定它们之间的差异,因而无法选择更合适的用户集来执行任务。

近年来,风险作为访问控制的一个重要方面引起了人们的重视,如文献[8-9]在效用概念的基础上用风险平衡系统的安全与收益,文献[10-11]将风险用于授权决策。在风险评估上,基于模糊理论的风险评估是重要的风险评估方法之一,如文献[12-13]给出了模糊风险分析的方法,文献[14]提出了信息系统风险的模糊综合评判模型。资源访问权限授予主体,主体以获得的授权访问资源可能对系统机密性、完整性和可用性等安全属性产生影响,这种由于授权产生的风险称之为授权风险。文献[8]指出"一定安全级的主体访问一定敏感级的客体,存在导致信息泄漏的风险",文献[9]指出"不同的权限有不同的风险级"。不同的用户执行同一授权产生的风险存在差异,如资深注册会计师执行会计任务的风险可能优于初级注册会计师。因此,分析不同的用户集执行任务权限集的聚集风险的差异,是满足敏感任务的安全需求的客观需要。

基金项目:国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2006AA01A113);山东省自然科学基金(the Natural Science Foundation of Shandong Province of China under Grant No.Y2008G28)。

作者简介:杨勇(1976-),男,硕士研究生,主要研究领域为安全策略与机制、访问控制;孙宇清(1967-),通讯作者,女,博士,副教授,硕士生导师,主要研究领域为安全策略与机制、系统安全、访问控制;周丽(1983-),女,硕士研究生,主要研究领域为安全策略与机制。

收稿日期:2008-10-22 修回日期:2009-01-12

提出基于风险的模糊安全策略,不仅用资质表达式限定了执行任务的用户数量和身份,而且量化了用户角色授权风险,给出了用户集执行一定角色集的风险评估模型。在讨论了给定用户集和风险阈值的安全策略的可满足性之后,给出了一个利用模糊用户-风险满足性检测算法判定给定用户集是否满足安全需求的应用实例。

2 基本概念与风险评估模型

2.1 基本概念

鉴于基于角色的访问控制(RBAC)现已在许多领域广泛应用,下面的讨论基于RBAC模型,用户的授权均通过角色来完成。

定义1(系统状态(System State)) 系统状态是指当前的用户、用户角色和角色权限授权关系的配置,表示为$<U,R,P,UR,RP>$的形式,其中U表示用户集,R表示角色集,P表示权限集,$UR=\{(u,r)|u\in U,r\in R\}$是用户角色授权关系,$(u,r)\in UR$表示$u$拥有角色$r$,$PR=\{(r,p)|p\in P,r\in R\}$是角色权限授权关系,$(r,p)\in PR$表示$r$包含权限$p$。一个用户角色配置可以被系统状态唯一确定,表示为$<U,UR>$。

定义2(风险等级集(Risk Levels)) 风险等级表示风险程度的大小,风险等级集可以表示为$RL=\{l_1,l_2,\cdots,l_k\}$的形式,其中,$i=1,2,\cdots,k$,$l_i$表示风险等级且满足$l_i<l_{i+1}$,即等级为$l_i$的风险小于等级为$l_{i+1}$的风险。

定义3(风险度向量(Risk Level Vector)) 风险度向量是对特定对象的风险评价,表示成含有k个元素的向量形式,形如$\boldsymbol{R}_{RL}(x)=(\mu_{l_1}(x),\mu_{l_2}(x),\cdots,\mu_{l_k}(x))$,其中$x$是被评价对象,$\mu_{l_i}(x)$表示对该对象的风险评价隶属于风险等级$l_i\in RL$的程度(即隶属度[15])。

例1 $RL=\{l_1,l_2,l_3,l_4,l_5\}=\{VL,L,M,H,VH\}$,5个风险等级分别为风险很低、低、中等、高和很高。风险度向量$\boldsymbol{R}_{RL}(x)=(0,0.4,0.6,0,0)$,表示对$x$的风险评价隶属于5个风险等级$VL$、$L$、$M$、$H$和$VH$的程度依次是0、0.4、0.6、0和0。

定义4(用户角色授权风险(User-Role Risk)) 用户角色授权风险(简称为*U-R*风险)是指授权角色r由单一用户u承担所产生的风险,表示为k维风险度向量的形式,形如$\boldsymbol{R}_{RL}(u,r)=(\mu_{l_1}(u,r),\mu_{l_2}(u,r),\cdots,\mu_{l_k}(u,r))$,其中,$(u,r)$是被评价对象,$\mu_{l_i}(u,r)$表示隶属于等级$l_i\in RL$的程度。

根据经验或用户属性,专家可以独立给出用户u承担角色r的风险等级的评价,表示为$R(u,r)$。风险度向量$\boldsymbol{R}_{RL}(u,r)$是多个独立风险等级评价的综合形式,它是采用了统计的方法,将被评价对象隶属于风险等级l_i的次数所占总评价次数的比重作为l_i的隶属度。

例2 $RL=\{VL,L,M,H,VH\}$,用户u_1拥有角色r_1,风险等级评价$R(u_1,r_1)$的统计结果如表1所示,总评价次数为10,故$\boldsymbol{R}_{RL}(u_1,r_1)=(1/10,4/10,4/10,1/10,0/10)=(0.1,0.4,0.4,0.1,0)$。

表1 风险等级评价统计表

风险等级	*VL*	*L*	*M*	*H*	*VH*
评价次数	1	4	4	1	0

可以根据一定的隶属原则,计算被评价对象x的综合风险评价$\boldsymbol{R}_{RL}(x)$的等级,表示为$f(x)$。

原则1(最大-最高隶属原则) 设$\boldsymbol{R}_{RL}(x)$的元素最大值是max,若l_h是其中对应的最高的风险等级,则$f(x)=l_h$。根据该原则,上述例子$\boldsymbol{R}_{RL}(u_1,r_1)$的等级为$f(u_1,r_1)=M$。

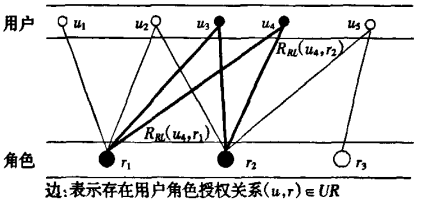
2.2 *Us-Rs*风险及评估模型

定义5(用户集-角色风险(Users-Role Risk)) 用户集-角色风险(简称为*Us-R*风险)是指角色r由给定$Us(Us\subseteq U)$中拥有角色$r(r\subseteq R)$的用户一起承担所产生的风险,它是多个用户角色授权风险$\boldsymbol{R}_{RL}(u,r)$,$u\in Us$的合集,表示为k维风险度向量的形式,形如$\boldsymbol{R}_{RL}(Us,r)=(\mu_{l_1}(Us,r),\mu_{l_2}(Us,r),\cdots,\mu_{l_k}(Us,r))$。

定义6(*Us-Rs*风险(Users-Roles Risk)) *Us-Rs*风险是指给定用户集$Us(Us\subseteq U)$中的用户承担角色集$Rs(Rs\subseteq R)$中的角色所产生的风险,它是多个*Us-R*风险$\boldsymbol{R}_{RL}(Us,r)$,$u\in Rs$的合集。表示为$k$维风险度向量的形式,形如$\boldsymbol{R}_{RL}(Us,Rs)=(\mu_{l_1}(Us,Rs),\mu_{l_2}(Us,Rs),\cdots,\mu_{l_k}(Us,Rs))$。其风险等级,表示为$f(Us,Rs)$。

将分析满足一定资质约束的用户集Us的*Us-Rs*风险(如例3),资质及其满足性见第3.1节。

例3 $U=\{u_1,u_2,u_3,u_4,u_5\}$,$Rs=\{r_1,r_2\}$,要求$Rs$由两个同时拥有角色$r_1$和$r_2$的用户执行,用户角色授权关系如图1所示。$\{u_2,u_3\}$、$\{u_3,u_4\}$或$\{u_2,u_4\}$均满足约束,但是这些用户集的*Us-Rs*风险可能不同,其中,$Us=\{u_3,u_4\}$的*Us-Rs*风险是图中粗线表示的边上的值$\boldsymbol{R}_{RL}(u_3,r_1)$、$\boldsymbol{R}_{RL}(u_3,r_2)$、$\boldsymbol{R}_{RL}(u_4,r_1)$和$\boldsymbol{R}_{RL}(u_4,r_2)$的合集。



边:表示存在用户角色授权关系$(u,r)\in UR$

边上的值:表示u_i承担r_j的用户角色授权风险$R_{RL}(u_i,r_j)$

图1 用户角色授权关系(UR)

下面,给出*Us-Rs*风险的评估模型。

假定风险等级集$RL=\{l_1,l_2,\cdots,l_k\}$,用户集$Us(Us\subseteq U)$是给定用户集,角色集$Rs=\{r_j|j=1,2,\cdots,m\}(Rs\subseteq R)$。采用模糊综合评估法计算*Us-Rs*风险,该方法综合了层次分析法(AHP)[16]和模糊评估法的优点。其计算过程如下:

(1)确定评价因子

*Us-Rs*风险的评价因子可分为两层(表2),第一层是主因

表2 基于层次的*Us-Rs*风险的评价因子

*Us-R*风险(主因子)	*U-R*风险(次因子)
$\boldsymbol{R}_{RL}(Us,r_1)$	$\boldsymbol{R}_{RL}(u_{h_1}^1,r_1)$
	…
	$\boldsymbol{R}_{RL}(u_{h_1}^a,r_1)$
$\boldsymbol{R}_{RL}(Us,r_2)$	$\boldsymbol{R}_{RL}(u_{h_2}^1,r_2)$
	…
	$\boldsymbol{R}_{RL}(u_{h_2}^b,r_2)$
…	…
$\boldsymbol{R}_{RL}(Us,r_m)$	$\boldsymbol{R}_{RL}(u_{h_m}^1,r_m)$
	…
	$\boldsymbol{R}_{RL}(u_{h_m}^q,r_m)$

子,由 m 个不同角色 r_j 的 $\boldsymbol{R}_{RL}(Us,r_j)$ 组成,第二层是次因子,由执行角色 r_j 的多个用户角色授权风险 $\boldsymbol{R}_{RL}(u_{r_j}^{l},r_j)$ 组成,其中 $u_{r_j}^{l}$ 表示该用户是执行角色 r_j 的第 l 个用户。为确定相关的用户角色授权风险,根据配置<U,UR>和用户集 Us,对于 $\forall r_j\in Rs$ 和 $\forall u\in Us$,若$(u,r_j)\in UR$,则 $\boldsymbol{R}_{RL}(u,r_j)$ 是 $\boldsymbol{R}_{RL}(Us,r_j)$ 的次因子。

(2)构造主因子的权重矩阵

根据标度理论,采用 1-9 标度(表 3),专家对主因子两两比较,构造判断矩阵 $\boldsymbol{A}=(a_{ij})_{m\times m}$,$a_{ij}>0$,$a_{ii}=1$,$a_{ji}=1/a_{ij}$。然后,确定主因子权重,即计算重要性排序向量:$\boldsymbol{AW}=\lambda_{\max}\boldsymbol{W}$,其中 $\lambda_{\max}$ 为最大特征根,$\boldsymbol{W}$ 为归一化特征向量。为避免逻辑上的误差,需要进行随机一致性检验:$CR=(\lambda_{\max}-m)/(m-1)RI$,$m$ 为判断矩阵的阶数,RI 为随机一致性指标,可根据判断矩阵阶数查表得到,若 $CR<0.10$,将特征向量 $\boldsymbol{W}=(w_1,w_2,\cdots,w_m)$ 作为主因子权重矩阵,否则修改判断矩阵。

表 3 1~9 标度的含义

标度	1	3	5	7	9
对比重要程度	同等重要	稍微重要	明显重要	强烈重要	极为重要
备注	2/4/6/8 等其他标度的含义介于上述判断之间				

(3)计算主因子

对于 $\forall r_j\in Rs$,计算 $\boldsymbol{R}_{RL}(Us,r_j)$。若 Us 中有 $q\in N$ 个用户拥有授权的角色 r_j,则 r_j 的 $\boldsymbol{R}_{RL}(Us,r_j)$ 是 $\boldsymbol{R}_{RL}(u_{r_j}^{l},r_j)$,$l=1,2,\cdots,q$ 的聚集,其计算过程如下:

如果 $q=1$,则 $\boldsymbol{R}_{RL}(Us,r_j)=\boldsymbol{R}_{RL}(u_{r_j}^{l},r_j)$;否则,$q$ 个风险度向量 $\boldsymbol{R}_{RL}(u_{r_j}^{l},r_j)$,$l=1,2,\cdots,q$ 进行模糊或运算(公式(1))得到 $\boldsymbol{R}_{RL}^{*}(Us,r_j)$,归一化后的结果即为 $\boldsymbol{R}_{RL}(Us,r_j)$。

$$\boldsymbol{R}_{RL}^{*}(Us,r_j)=\bigvee_{l=1,2,\cdots,q}\boldsymbol{R}_{RL}(u_{r_j}^{l},r_j)=\begin{pmatrix}\mu_{t_1}(u_{r_j}^{1},r_j)\vee\mu_{t_1}(u_{r_j}^{2},r_j)\vee\cdots\vee\mu_{t_1}(u_{r_j}^{q},r_j)\\ \vdots\\ \mu_{t_k}(u_{r_j}^{1},r_j)\vee\mu_{t_k}(u_{r_j}^{2},r_j)\vee\cdots\vee\mu_{t_k}(u_{r_j}^{q},r_j)\end{pmatrix}^{\mathrm{T}}\quad(1)$$

(4)计算 Us-Rs 风险

采用公式(2)将主因子权重矩阵 $\boldsymbol{W}$ 与主因子模糊矩阵 $\boldsymbol{R}=(\boldsymbol{R}_{RL}(Us,r_1),\boldsymbol{R}_{RL}(Us,r_2),\cdots,\boldsymbol{R}_{RL}(Us,r_m))^{\mathrm{T}}$ 进行模糊运算,得到 $\boldsymbol{R}_{RL}^{*}(Us,Rs)$,其中算子。采用最大-代数积模型,即 $\mu_{t_i}(Us,Rs)=\vee(w_j\cdot\mu_{t_i}(Us,r_j))$,$j=1,2,\cdots,m$,$i=1,2,\cdots,k$。归一化处理后的结果即为 $\boldsymbol{R}_{RL}(Us,Rs)$,根据原则 1,计算可得 $f(Us,Rs)$。

$$\boldsymbol{R}_{RL}^{*}(Us,Rs)=\boldsymbol{W}\circ\boldsymbol{R}=(w_1,w_2,\cdots,w_m)\circ\begin{pmatrix}\boldsymbol{R}_{RL}(Us,r_1)\\ \vdots\\ \boldsymbol{R}_{RL}(Us,r_m)\end{pmatrix}=$$

$$\begin{pmatrix}(w_1\cdot\mu_{t_1}(Us,r_1))\vee\cdots\vee(w_m\cdot\mu_{t_1}(Us,r_m))\\ \vdots\\ (w_1\cdot\mu_{t_k}(Us,r_1))\vee\cdots\vee(w_m\cdot\mu_{t_k}(Us,r_m))\end{pmatrix}^{\mathrm{T}}\quad(2)$$

设用户集$|X|=n$,角色集$|Rs|=m$,$|RL|=k$,$m,n,k\in N$,则复杂度为 $O(m^2+m*n*k+m^2*k)$,若 $n=\max(n,m,k)$,则复杂度约为 $O(n^3)$。

例 4 $RL=\{ML,L,M,H,MH\}$,$UR=\{(u_1,r_1),(u_2,r_2),(u_3,r_2),(u_4,r_4)\}$,$\boldsymbol{R}_{RL}(u_1,r_1)=(0.1,0.6,0.2,0.1,0)$,$\boldsymbol{R}_{RL}(u_2,r_2)=(0.3,0.3,0.4,0,0)$,$\boldsymbol{R}_{RL}(u_3,r_2)=(0.3,0.5,0.2,0,0)$,$\boldsymbol{R}_{RL}(u_4,r_4)=(0.2,0.3,0.4,0.1,0)$。$Us=\{u_1,u_2,u_3\}$,$Rs=\{r_1,r_2\}$,求 $f(Us,Rs)$。

第 1 步,确定评价因子,其主因子是 $\boldsymbol{R}_{RL}(Us,r_1)$ 和 $\boldsymbol{R}_{RL}(Us,r_1)$,前者的次因子是 $\boldsymbol{R}_{RL}(u_1,r_1)$,后者的次因子是 $\boldsymbol{R}_{RL}(u_2,r_2)$ 和 $\boldsymbol{R}_{RL}(u_3,r_2)$;第 2 步,确定主因子权重矩阵 $\boldsymbol{W}$,这里假定 $\boldsymbol{W}=(0.67,0.33)$;第 3 步,计算主因子 $\boldsymbol{R}_{RL}(Us,r_1)$ 和 $\boldsymbol{R}_{RL}(Us,r_2)$,其中 $\boldsymbol{R}_{RL}(Us,r_1)=\boldsymbol{R}_{RL}(u_1,r_1)$,运用公式(1)计算可得 $\boldsymbol{R}_{RL}^{*}(Us,r_2)=\boldsymbol{R}_{RL}(u_2,r_2)\vee\boldsymbol{R}_{RL}(u_3,r_2)=(0.3,0.5,0.4,0,0)$,归一化后得 $\boldsymbol{R}_{RL}(Us,r_2)=(0.25,0.42,0.33,0,0)$;第 4 步,运用公式(2)计算得:

$$\boldsymbol{R}_{RL}^{*}(Us,Rs)=\boldsymbol{W}\circ\boldsymbol{R}=(0.67,0.33)\circ\begin{pmatrix}\boldsymbol{R}_{RL}(Us,r_1)\\ \boldsymbol{R}_{RL}(Us,r_2)\end{pmatrix}=$$

$$(0.67,0.33)\circ\begin{pmatrix}0.1 & 0.6 & 0.2 & 0.1 & 0\\ 0.25 & 0.42 & 0.33 & 0 & 0\end{pmatrix}=$$

$$(0.01,0.40,0.13,0.07,0)$$

归一化后 $\boldsymbol{R}_{RL}(Us,Rs)=(0.02,0.66,0.21,0.12,0)$,根据原则 1,由于 $\max(\boldsymbol{R}_{RL}(Us,Rs))=\mu_L(Us,Rs)=0.66$,故 $f(Us,Rs)=L$。

3 模糊安全策略

资质和风险阈值是模糊安全策略的重要组成部分,首先给出它们的定义并讨论其满足性。

3.1 资质和风险阈值

将操作符¬,Π,Ш,⊗,+用于资质表达式,其中,一元操作符号¬表示非、+表示一个或多个,二元操作符Ш表示或,Π表示与,⊗表示两侧分别成立且不存在交。¬优先级最高,其他同。

定义 7(资质(Qualification)) 资质是指对执行任务的用户集的用户数量和用户身份的约束,其表达式用 ϕ 表示,定义如下:

(1)原子表达式:原子表达式是指任意下列 4 种形式之一:角色 r(表示用户集的共同身份)、关键字 any(表示任意用户)、特定的用户列表 $S(S\subseteq U)$和¬ r(表示不拥有角色 r 的任意用户),用 ϕ_0 表示。例如:manager、any、{Alice,Bob}和¬ manager,分别表示要求用户拥有 manager 角色、是任何用户、是 Alice 或 Bob 和不拥有 manager 角色的任何用户。

(2)资质表达式:资质表达式是指原子表达式或操作符¬,Π,Ш,⊗,+作用于原子表达式所形成的表达式。若 ϕ_1,ϕ_2 是资质表达式,则形如 $\phi_1\Pi\phi_2$、$\phi_1\text{Ш}\phi_2$、$\phi_1\otimes\phi_2$、ϕ_1^{+}、¬ ϕ_1 也是资质表达式。当¬,Π,Ш作用于原子表达式时,可形成单一资质表达式,要求用户数为 1。

例如:$(r_1\text{Ш}r_2)\otimes r_3\otimes r_4$ 要求用户集有 3 个用户,一个有 r_1 或 r_2 角色,一个有 r_3 角色,一个有 r_4 角色;$r_1\otimes r_2\otimes(r_3\Pi r_4)^{+}$ 要求用户集有 3 个或 3 个以上用户,一个有 r_1 角色,一个有 r_2 角色,一个或多个同时有 r_3 和 r_4 角色。不遵循操作符含义或任何系统状态下都不能满足的资质表达式是不合法的表达式,如 $(r_1\otimes r_2)\Pi r_3$、¬ any、{Alice,Bob}Π{Peter}、$r_1\Pi$¬ r_1 等。

定义 8(风险阈值(Risk threshold)) 风险阈值是给定的可接受的风险等级的上界,用 *threshold* 表示,*threshold* $\in RL$,缺省值是最大风险等级。

定义 9(资质的满足性(Satisfaction of Qualification)) 给定

一个配置<U,UR>,说用户集 Us 在<U,UR>下满足资质表达式 ϕ 当且仅当下列之一成立:

(1)ϕ 是一个角色 r,Us 是一个单一用户集$\{u\}$使$(u,r)\in UR$;

(2)ϕ 是一个关键词 any,Us 是一个单一用户集$\{u\}$使 $u\in U$;

(3)ϕ 是一个用户集 S,Us 是一个单一用户集$\{u\}$使 $u\in S$;

(4)ϕ 是$\neg\ \phi_0$形式,ϕ_0是一个单一资质表达式,Us 是一个不满足 ϕ_0的单一用户集$\{u\}$;

(5)ϕ 是 ϕ_0^+形式,ϕ_0是一个单一资质表达式,Us 是一个非空用户集,其每个用户 $u\in Us$,$\{u\}$满足 ϕ_0;

(6)ϕ 是 $\phi_1\amalg\phi_2$的形式,Us 满足 ϕ_1或 Us 满足 ϕ_2;

(7)ϕ 是 $\phi_1\amalg\phi_2$的形式,Us 满足 ϕ_1且满足 ϕ_2;

(8)ϕ 是 $\phi_1\otimes\phi_2$的形式,存在 Us_1和 Us_2使 $Us_1\cup Us_2=Us$,$Us_1\cap Us_2=\Phi$,Us_1满足 ϕ_1且 Us_2满足 ϕ_2。

如果用户集 Us 满足资质 ϕ,则称用户集 Us 是资质满足用户集。

资质表达式中的原子表达式 ϕ_0可以被看作是特殊角色,其中any、{Alice}、$\neg\ r$ 分别看作共有角色、角色 Alice 和非 r 的共有角色。若用户集 Us 满足 ϕ,将满足 ϕ 的相关的原子表达式形成的集合作为角色集 Rs,用 2.2 节的 ***Us-Rs*** 风险评估模型,计算可得用户集 Us 关于 ϕ 的 ***Us-Rs*** 风险 $\boldsymbol{R}_{RL}(Us,Rs)$,为直观,记为 $\boldsymbol{R}_{RL}^*(Us,\phi)$,其风险等级记为 $f(Us,\phi)$。

例如:$\phi=(r_1\amalg r_2)\otimes r_3$,若用户集 Us 满足 $r_2\otimes r_3$,则 $f(Us,\phi)$表示用户集 Us 关于 ϕ 的 ***Us-Rs*** 风险的等级,其中 $Rs=\{r_2,r_3\}$。

当 ϕ_0是 any、$\neg\ r$ 或特定用户集 S 时,对满足 ϕ_0的用户的要求没有差异,这些不同用户的用户角色授权风险 $\boldsymbol{R}_{RL}(Us,\phi_0)$对 ***Us-Rs*** 风险的影响可以忽略。因此,当风险阈值取 $l_h\in RL$ 时,取风险度向量 $\boldsymbol{R}_{RL}(Us,\phi_0)$的第 h 个元素为 1,其余为 0,如 $RL=\{ML,L,M,H,VH\}$,风险阈值为 M,则取 $\boldsymbol{R}_{RL}(Us,\phi_0)=(0,0,1,0,0)$。

定义 10(风险阈值的满足性(Satisfaction of Risk threshold)) 资质满足用户集 Us 满足风险阈值当且仅当用户集 Us 的 $f(Us,\phi)\leqslant threshold$。

特别地,当 $threshold$ 取 RL 中的最大风险等级时,任意的资质满足用户集 Us 的 $f(Us,\phi)$都满足风险阈值。如果资质满足用户集 Us 满足风险阈值,则称用户集 Us 是风险满足用户集,显然,后者是前者的子集。

3.2 模糊安全策略

定义 11(模糊安全策略(Fuzzy Security Policy)) 一个模糊安全策略形如 $fsp<P_s,\phi,threshold>$,其中,P_s($P_s\subseteq P$)表示任务包含的权限集;ϕ 是资质表达式,$threshold$ 是风险阈值。它的含义是只有覆盖权限的用户集 Us'有一个满足资质和风险阈值的用户子集 Us 才能被选择执行任务。

模糊安全策略的表达比较丰富,下面给出几个表达的例子,其中 $RL=\{ML,L,M,H,VH\}$:

(1)$fsp_1<P_{s1}(manager\amalg audit)\otimes clerk,L>$,要求执行任务$P_{s1}$的用户集 Us'包含的用户集 Us:由一名管理员或审计员和一名职员组成,且 ***Us-Rs*** 风险的等级不超过 L。

(2)$fsp_2<P_{s2}(manager\otimes Engineer\otimes Engineer^+,VH)>$,要求执行任务 P_{s2}的用户集 Us'包含的用户集 Us:由一名管理员和两名或两名以上的工程师组成。

定义 12(策略的可满足性(Policy Satisfiability)) 一个模糊安全策略是可满足的,当且仅当在当前系统状态下至少存在一个覆盖任务权限集 Ps 的用户集 Us'包含满足资质和风险阈值的用户子集 Us。

4 策略的可满足性检测

策略的可满足性检查的核心是在给定资质、风险阈值和系统状态下,确定是否存在一个用户集 Us 是风险满足用户集,其基本问题是模糊用户-风险满足性(FURSAT)问题:即判定一个给定用户集 Us 是否是风险满足用户集。余下部分将讨论 FURSAT 问题,其他问题超出该文范围。

4.1 资质表达式的规范式

一般形式的资质表达式的用户-资质满足性检测问题是 NP 完全问题[7],为使其成为 P 问题,给出资质表达式的规范形式。

定义 13(资质表达式的规范式(Canonical Form)) 一级范式(1CF)是 t 或 t^+,t 是单一资质表达式的形式,二级范式(2CF)是包含一个或多个 1CF 并用$\otimes$连接的形式,三级范式(3CF)是包含一个或多个 2CF 并用$\amalg$连接的形式。

例如:$\phi=(r_1\amalg r_2)\otimes r_3\otimes(r_4\amalg r_5)$是一个 2CF,$\phi=((r_1\amalg r_2)\otimes r_3))\amalg((r_4\amalg r_5)\otimes r_6)$是一个 3CF。

引理 1 给定规范的资质表达式 ϕ 和风险阈值 $threshold$,判断用户集 Us 是否是风险满足用户集能够在多项式时间内完成。

证明 若 ϕ 是 3CF,则用$\amalg$或$\amalg$连接若干子表达式 2CF,每个 2CF 表达式可以分解为用$\otimes$连接一个或多个单一资质条件表达式,易知每个单一资质表达式的满足性判定可在多项式时间内完成(根据定义 9),所以检查一个用户集 Us 在配置<U,UR>下是否满足 ϕ 能够在多项式时间完成。若用户集 Us 是资质满足用户集,根据 1.2 节可知计算用户集 Us 关于 ϕ 的风险等级 $f(Us,\phi)$可在多项式时间完成,故判定用户集 Us 是否满足资质表达式且 $f(Us,\phi)$满足风险阈值能够在多项式时间内完成。

4.2 模糊用户-风险满足性检测算法

FURSAT 检测算法:给定系统状态、模糊安全策略和用户集 Us,判定 Us 是否是风险满足用户集,其主要步骤如下:

(1)构造 ϕ 的语法树 T。原子表达式 ϕ_0或 ϕ_0^+作为叶节点(Leaf),连接形成子表达式的二元操作符$\amalg$$\amalg$$\otimes$作为中间节点(node)。

(2)计算 ϕ 的语法树 T,判定 Us 是否资质满足用户集。在<U,UR>下,采用自底向上的方法,从每个叶节点开始,计算满足每个原子表达式的 Us 的所有子集,对于 T 中的每个中间节点,计算满足以该节点为根的子表达式的用户集并标记到节点上,直到 T 的根。若根标记的用户集存在且等于 Us,则 Us 是资质满足用户集,否则 Us 不是资质满足用户集,算法结束。

(3)若 $threshold$ 是 RL 的最大风险等级,则用户集 Us 也是风险满足用户集,算法结束,否则进入(4)。

(4)根据计算得到用户集 Us 和满足 ϕ 所对应的角色集 Rs,采用 1.2 节的 ***Us-Rs*** 风险评估模型计算用户集 Us 关于 ϕ 的风险等级 $f(Us,\phi)$。

(5)若$f(Us,\phi)\leqslant threshold$成立,则用户集$Us$是风险满足用户集。

5 应用实例分析

给出一个应用实例分析。假定组织为敏感任务陈述了模糊安全策略,管理者希望知道当前系统状态下候选的用户集Us是否满足资质与风险阈值,可以被选择参与执行任务。

例5 一个财务工作要求执行任务的用户必须有两个用户,其中一名是主管或会计,另一名是出纳,每个人都是公司职员,风险阈值为l_2。$RL=\{ML,L,M,H,VH\}$,模糊安全策略$fsp_1<P,\phi,L>$,其中$\phi=((\text{manager}\ \Pi\ \text{clerk})\ \amalg\ (\text{accoutant}\ \Pi\ \text{clerk}))\otimes(\text{cashier}\ \Pi\ \text{clerk})$,给定用户集是{Alice,Carl},{Alice,Peter}和{Bob,Carl},要求判定哪个是风险满足用户集。现有其他有关的情况及判定过程描述如下:

(1)系统状态

$UR=\{$(Alice,manager),(Tom,accountant),(Peter,cashier),(Carl,cashier),(Alice,Clerk),(Bob,Clerk),(Peter,Clerk),(Carl,Clerk),(Tom,Clerk),$\cdots\}$

(2)用户角色授权风险

R_{RL}(Alice,manager)=(0.6,0.2,0.2,0,0)

R_{RL}(Tom,accountant)=(0.2,0.7,0.1,0,0)

R_{RL}(Peter,cashier)=(0.1,0.2,0.7,0,0)

R_{RL}(Carl,cashier)=(0.1,0.2,0.5,0.2,0)

R_{RL}(Alice,clerk)=(0.8,0.2,0,0,0)

R_{RL}(Bob,clerk)=(0.75,0.25,0,0,0)

R_{RL}(Peter,clerk)=(0.5,0.3,0.2,0,0)

R_{RL}(Carl,clerk)=(0.7,0.2,0.1,0,0)

R_{RL}(Tom,clerk)=(0.8,0.2,0,0,0)

(3)利用FURSAT检测算法的判定过程如下:

①取$\otimes$为根节点,构造ϕ的语法树T。

②取用户集Us={Alice,Carl},从语法树T的叶节点开始,采用自底向上匹配,在节点上标记满足以该节点为根ϕ的的子表达式的用户集Us的所有子集,直到根(如图2)。根的标记用户集为{Alice,Carl},故该用户集是资质满足用户集。

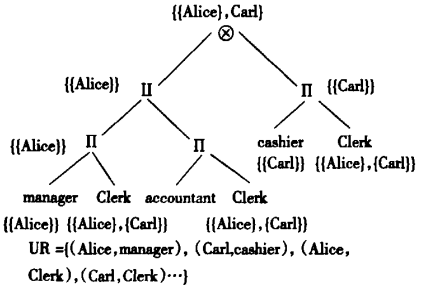


图2 语法树T和用户集Us={Alice,Carl}的自底向上匹配图

③由于$threshold\neq VH$,进入下一步。

④用户集Us={Alice,Carl}承担资质表达式中的角色集Rs={manager,cashier,clerk},主因子是$R_{RL}(Us,\text{manager})$、$R_{RL}(Us,\text{cashier})$和$R_{RL}(Us,\text{clerk})$,其次因子分别是$R_{RL}$(Alice,manager)、$R_{RL}$(Carl,cashier)、$R_{RL}$(Alice,clerk)和$R_{RL}$(Carl,clerk)。计算可得$R_{RL}(Us,\text{manager})=R_{RL}$(Alice,manager),$R_{RL}(Us,\text{cashier})=R_{RL}$(Carl,cashier),$R_{RL}(Us,\text{clerk})=R_{RL}$(Alice,clerk)$\vee$ R_{RL}(Carl,clerk)=(0.73,0.18,0.09,0,0),主因子模糊矩阵R:

$$R=(R_{RL}(Us,Manager),R_{RL}(Us,Cashier),R_{RL}(Us,Clerk))^{T}=\begin{pmatrix}R_{RL}(Us,Manager)\\R_{RL}(Us,Cashier)\\R_{RL}(Us,Clerk)\end{pmatrix}=\begin{pmatrix}0.60&0.20&0.20&0&0\\0.10&0.20&0.50&0.2&0\\0.73&0.18&0.09&0&0\end{pmatrix}$$

设权重矩阵W=(0.43,0.43,0.14),用公式(2)计算可得$R^{*}_{RL}(Us,Rs)=W\circ R$=(0.26,0.09,0.22,0.09,0),归一化后得$R_{RL}(Us,Rs)$=(0.39,0.14,0.33,0.14,0)。根据原则1,由于$\max(R_{RL}(Us,Rs))$=0.39=$\mu_{VL}(Us,Rs)$,故$f(Us,Rs)=VL$,即f({Alice,Carl},ϕ)=VL。

⑤f({Alice,Carl},ϕ)=$VL<L$,故{Alice,Carl}是风险满足用户集。

同理,当取用户集Us={Alice,Peter}时,该用户集是资质满足用户集,Rs={manager,cashier,clerk},$R_{RL}(Us,Rs)$=(0.35,0.12,0.41,0.12,0),根据原则1,由于$\max(R_{RL}(Us,Rs))$=0.41=$\mu_{M}(Us,Rs)$,故$f(Us,Rs)=M$,即f({Alice,Peter},ϕ)=$M>L$,故{Alice,Peter}不是风险满足用户集;当取用户集Us={Bob,Carl}时,不是资质满足用户集,故不是风险满足用户集。

6 结论

职责分离是访问控制的基本安全原则之一,提出的模糊安全策略对职责分离进行了扩展,不仅限定了执行敏感任务的用户的数量和身份,而且定量分析了满足这些约束的用户集执行多项授权的聚集风险。在分析了资质的满足性基础上,讨论了给定风险阈值的模糊安全策略的可满足性,并给出了判定用户集的是否满足风险阈值的算法。在当前系统状态下,组织机构可以利用该算法判定给出的候选用户集是否满足资质与风险约束,从而选择符合敏感任务安全需求的用户集参与任务执行。下一步,将研究当前系统状态下的资质满足用户集存在性问题及基于风险的授权。

参考文献:

[1] Clark D D,Wilson D R.A comparision of commercial and military computer security policies[C]//Proc of the 1987 IEEE Symposium on Security and Privacy.[S.l.]:IEEE Computer Society Press,1987:184-194.

[2] Nash M J,Poland K R.Some conundrums concerning separation of duty[C]//Proc of IEEE Symposium on Research in Security and Privacy,1990:201-209.

[3] Sandhu R S,Coyne E J,Feinstern H L,et al.Role-based access control models[J].IEEE Computer,1996,29(2):38-47.

[4] Gligor V D,Gavrila S I,Ferraiolo D F.On the formal definition of separation-of-duty policies and their composition[C]//Proc of IEEE Symposium on Research in Security and Privacy,1998:172-183.

[5] Crampton J.Specifying and enforcing constraints in role-based access control[C]//Proc of the 8th ACM Symposium on Access Control Models and Technologies SACMAT 2003,Como,Italy,2003:43-50.

[6] Tidswell J,Jaeger T.An access control model for simplifying constraint expression[C]//Proc of ACM Conference on Computer and Communications Security,2000:154-163.

(下转111页)

能够很好地应用于这种环境。

6 结束语

提出了一个高效的基于身份的公开可验证加密签名方案。在BDH问题是困难的假设下,运用随机预言模型证明了该方案的安全性。新方案具有公开可验证性、保密性、不可伪造性、不可否认性与前向安全等安全特性并且能够将签名的验证和消息的恢复分别独立进行。与已有的一些典型的基于身份的签密方案相比,该文方案效率更高。

参考文献:

[1] Zheng Y.Digital signcryption or how to achieve cost(signature & encryption<<cost(signature)+cost(encryption)[C]//Kaliski B S.LNCS 1294:Advances in Cryptology-CRYPTO'97.Berlin:Springer-Verlag,1997:165-179.

[2] Zheng Y.Signcryption and its applications in efficient public key solutions[C]//LNCS 1397:ISW'97.[S.l.]:Springer-Verlag,1998:291-312.

[3] Shamir A.Identity-based cryptosystems and signature schemes[C]//Blakley G R,Chaum D.LNCS 196:Advances in Cryptology-CRYPTO'84.Berlin:Springer-Verlag,1984:47-53.

[4] Boneh D,Franklin M.Identity-based encryption from the wepairing[J].SIAM Journal of Computing,2003,32(3):586-615.

[5] Malone-Lee J.Identity based signcryption,Report 2002/098[R].Cryptology ePrint Archive,IACR,2002.

[6] Libert B,Quisquater J.A new identity based signcryption schemes from pairings[C]//Proceedings of the 2003 IEEE Information Theory Workshop,France,2003:155-158.

[7] Boyen X.Multipurpose identity-based signcryption:A Swissarmy knife for identity-based cryptography[C]//LNCS 2729:Advances in Cryptology,CRYPTO 2003.Berlin:Springer-Verlag,2003:383-399.

[8] Chouw S S M,Yiu S M,Hui L C K,et al.Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity[C]//LNCS 2971:Advances in Information Security and Cryptology,ICISC'03.Berlin:Springer-Verlag,2004:352-369.

[9] 李发根,胡予濮,李刚.一个高效的基于身份的签密方案[J].计算机学报,2006,29(9):1641-1647.

[10] Yuen T H,Wei V K.Fast and proven secure blind identity-based signcryption from pairings[C]//LNCS 3376:Advances in Cryptology,CR2005.Berlin:Springer-Verlag,2005:305-322.

(上接86页)

[7] Li N,Wang Q.Beyond separation of duty:An algebra for specifying high-level security policies[C]//Proc of ACM Conference on Computer and Communications Security(CCS),2006.

[8] Dimmock N,Belokosztolszki A,Eyers D,et al.Using trust and risk in role-based access control policies[C]//Proc Symposium on Access Control Models and Technologies(SACMAT),2004:156-162.

[9] Zhang Lei,Brodsky A,Jajodia S.Toward information sharing:Benefit And Risk Access Control(BARAC)[C]//7th IEEE International Workshop on Policies for Distributed Systems and Networks(POLICY'06),2006:45-53.

[10] Cheng P C,Rohatgi P,Keser C,et al.Fuzzy multi-level security:An experiment on quantified risk adaptive access control,IBM Research Report RC24190[R].2007.

[11] Nissanke N,Khayat E J.Risk based security analysis of permissions in RBAC[C]//2nd International Workshop on Security in Information Systems,Porto,Portugal,2004.

[12] Huang Choug fu.Concepts and methods of fuzzy risk analysis[C]//Proc of the 1st China-Japan Conference on Risk Assessment and Management.[S.l.]:Beijing:International Academic Publishers,1998:12-23.

[13] 沈国柱.风险模糊分析法[J].系统工程与电子技术,2000,22(10):90-93.

[14] 肖龙,戴宗坤.信息系统风险的多级模糊综合评判模型[J].四川大学学报:工学版,2004,36(5):98-102.

[15] 彭祖赠.模糊数学及其应用[M].武汉:武汉大学出版社,2002.

[16] 许树柏.层次分析法原理[M].天津:天津大学出版社,1988.

(上接100页)

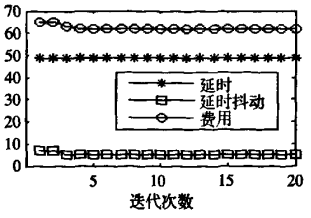


图2 组播树费用、延时和延时抖动随迭代次数变化曲线图

有进化意义的局部变异能使算法快速跳出局部最优解,并向好的方向进化。从而验证了算法是可行和有效的。

6 结束语

针对QoS组播路由问题,提出了一种改进的自适应变异二次蚁群算法,该算法采取自适应变异方法,借助节点使用计数器,引入二次蚁群搜索机制,减少了算法陷入局部极值的可能性,提高了算法的寻优能力和收敛速度。实验结果证明了上述结论。

参考文献:

[1] Wang Z,Crowcroft J.Quality-of-service routing for supporting multimedia applications[J].IEEE Journal of Selected Areas in Communications,1996,14(7):1228-1234.

[2] Dorigo M,Maniezzo V,Colorni A.The ant system:Optimization by a colony of cooperating agents[J].IEEE Transactions on Systems,Man,and Cybernetics B,1996,26(1):1-13.

[3] 杨莉,颜昕.基于蚂蚁代理的QoS多播路由算法[J].计算机科学,2007,34(1):52-56.

[4] 陈杰,张洪伟.基于自适应蚁群算法的QoS组播路由算法[J].计算机工程,2008,34(13):200-203.

[5] 王征应,石冰心.基于启发式遗传算法的QoS组播路由问题求解[J].计算机学报,2001,24(1):55-61.

FSP:一种基于风险的安全策略

作者： 杨勇， 孙宇清， 周丽， YANG Yong， SUN Yu-qing， ZHOU Li
作者单位： 山东大学计算机科学与技术学院,济南,250101
刊名： 计算机工程与应用 ISTIC PKU
英文刊名： COMPUTER ENGINEERING AND APPLICATIONS
年，卷(期)： 2010，46(13)
被引用次数： 0次

参考文献(16条)

1. Sandhu R S;coyne E J;Feinstern H L Role-based access control models 1996(02)

2. Nash M J;Poland K R Some conundrums concerning separation of duty 1990

3. Clark D D;Wilson D B A comparision of commercial and military computer security policies 1987

4. Zhang Lei;Brodsky A;Jajodia S Toward information sharing:Benofit And Risk Access Control(BARAC) 2006

5. Dimmock N;Belokosztolszki A;Eyers D Using trust and risk in role-based access control policies 2004

6. Li N;Wang Q Beyond separation of duty:An algebra for specifying high-level security pelicies 2006

7. Tidswell J;Jaeger T An access control model for simplifying constraint expression 2000

8. 许树柏 层次分析法原理 1988

9. 彭祖赠 模糊数学及其应用 2002

10. 肖龙;戴宗坤 信息系统风险的多级模糊综合评判模型[期刊论文]-四川大学学报(工学版) 2004(05)

11. 沈国柱 风险模糊分析法[期刊论文]-系统工程与电子技术 2000(10)

12. Hnang Choug fu Concepts and methods of fuzzy risk analysis 1998

13. Nissanke N;Khayat E J Risk besed security analysis of permissions in RBAC 2004

14. Cheng P C;Rohatgi P;Keser C Fuzsy multi-level security:An experiment on quantified risk adaptive access control,[IBM Research Report RC24190] 2007

15. Crampton J Spacifying and enforcing constraints in role-basod access control 2003

16. Gligor V D;Gavrfla S I;Ferraiolo D F On the formal definition of separation-of-duty policies and their composition 1998

相似文献(10条)

1. 学位论文 王婧 网格访问控制安全策略模型研究 2008

网格技术的发展，为信息资源的共享提供了更加完善的手段，企业在信息资源共享的同时也要阻止非授权用户对企业敏感信息的访问。访问控制的目的是保护企业在信息系统中存储和处理信息的安全。

网格系统访问控制策略是对进入网格系统用户的权限控制，其作用是对需要访问网格系统内数据的用户进行识别并检验其身份合法性，并对网格系统中发生的操作根据定制的安全策略来加以限制[1]。传统的安全标准和访问控制机制都无法满足网格计算系统特殊的安全需求。本文在深入分析基于动态安全级别的分级访问控制模型BLP(Bell—La Padula)[2]的基础上，结合网格计算系统动态特征，提出了一种新的网格访问控制安全策略模型GCSSMAC(Grid Computing SystemSecurity Model of Access Control)。该模型采用“区域自治，域间代理”原则，实现了虚拟组织成员通过成员代理安全访问管理域提供的实际网格计算服务的完整交互过程。在该模型中，“成员会话+VO角色+管理域角色”的组合唯一标识了网格环境下的合法用户，满足了网格计算系统的认证需求、通信保护需求、授权需求、数据完整性需求、数据保密性以及不可否认性需求等，充分体现出了该访问控制模型的安全性。除此之外，该模型克服了现有研究难以支持虚拟组织中高度灵活的共享关系定义和对共享资源的复杂性难以控制的缺陷，它可满足粗/细粒度访问控制和单点登录等应用需要，并可利用较为成熟的各种XML解析器实现语义精确的策略匹配和执行，体现了对灵活性、适应性、可伸缩性和可扩展性的良好支持，经理论分析及仿真实验验证，具有较强可行性。

2. 期刊论文 王立功.李晓瑛.李晓辉 网络服务器的访问控制安全策略 -焦作工学院学报(自然科学版)2002,21(3)

在计算机网络应用中,不可能通过任何纯技术的手段彻底消除安全风险.根据具体情况综合运用现有的安全手段是提高网络系统安全性的经济而有效的方法.提出了安全策略的概念,简述了主要技术性安全策略,指出访问控制策略是主要的安全策略,阐述了如何在服务器上实现访问控制策略.

3. 学位论文 陈晨 面向多域合作的安全策略分析与复合研究 2009

基于Web的资源共享和系统互操作是组织间进行合作的重要形式，确保合作组织信息系统的安全是保证共享资源安全性的重要方面。访问控制是确保

信息系统安全的关键技术，通过约束访问主体对被访问客体的行为以保护共享信息和资源。在实际应用中，访问控制依托安全策略来实施。安全策略是组织根据安全需求和业务目标制定的一系列涉及系统访问的许可或禁止的规定。在面向多域合作的应用中，如何有效地分析和整合不同组织的安全策略，在确保组织信息系统安全的同时，提高协同工作的效率，是一个至关重要的问题。

安全策略相似度是不同组织的安全策略，在访问主体、被访问客体或访问行为等安全约束上的相似程度，它比较的是不同安全策略之间权限分配的共同点和不同点。将策略相似度分析作为策略比较的前期步骤，能过滤掉相似度低的安全策略，返回高相似度值的策略集合，以便于细粒度的策略分析或提高安全策略复合的效率。在多域合作环境中，不同组织的资源受各自访问控制系统的保护，这就要求各组织在保护本地资源的同时，遵守其它组织的安全约束。策略复合的目的，就是有机地集成不同组织的安全策略，从而构建一个安全互信的协同工作环境，提高组织之间权限分配的效率。在策略复合领域中，合作策略是不同安全策略中，相应属性的相同属性值构成的共性安全策略。合作策略关注的是策略的属性复合，表达了合作组织之间共同的安全需求。对合作组织进行安全策略共性特征的抽取，以形成合作策略，能够保证组织合作的公平性，使合作组织在更大程度上共享资源，从而提高合作的效率。

在多域合作环境中，每个合作组织隶属于不同的管理机构，独立管理自己的资源和访问控制，并依据本地的安全需求和业务目标来定义安全策略，从而导致了安全策略的异构性。基于Web的多域合作环境通常使用XACML策略语言表示异构的访问控制策略。XACML是国际标准化组织制定的基于Web的安全策略描述语言标准之一，提供了完整的访问控制和授权系统标准，被广泛应用于Web环境中的安全策略表达，本文所做工作都基于XACML语言描述。当前对策略相似度的研究主要基于相同的概念层次结构，并使用相同的概念进行策略表达，没有考虑概念层次结构的异构性，不能处理更为普遍的策略异构情况。在策略复合领域，现有的安全策略复合方法大多关注于决策方案的复合，较少关注策略属性的复合，没有从合作策略共性特征抽取的角度强调合作组织之间的公平性，提高组织合作的效率。针对这两个问题，本文提出了异构安全策略相似度算法和安全策略共性特征抽取算法。本文主要工作和创新点如下：

在策略相似度分析方面，提出了异构安全策略相似度计算方法。算法首先通过语义映射技术，判断出不同安全策略中语义异构概念间的语义关系，并基于语义关系对异构概念层次结构进行结点合并。基于合并后的概念层次结构，通过概念的语义层次距离和合并前后的语义位置变化来计算安全策略的相似度值。算法对概念层次结构的合并，不仅能消除概念之间的语义异构，计算更为普遍的异构安全策略相似度值，而且基于语义层次距离和语义位置的变化计算相似度值更符合概念之间的语义差异，能够提高计算结果的准确性。在算法实验中，本文选取不同的概念层次结构和安全策略实例进行相似度计算，从而证明算法在运行效率上是可行的，在计算效果上能避免当前策略相似度研究中可能出现的相似度值相同的不准确现象。

在合作策略生成方面，提出了安全策略共性特征抽取算法。算法基于逻辑代数的形式进行安全策略表达，通过对安全规则的进一步范式分解和概念层次分解，获得每个属性只有单一属性值的原子规则。安全策略的共性特征依据原子规则中相应属性的属性值交集进行抽取。对安全规则进行范式分解和概念层次分解不仅能实现策略的属性复合，确保没有遗漏地抽取出不同安全策略的共同部分，而且对安全策略进行先分解再抽取的方法能有效提高策略共性特征抽取的效率。在算法实验中，通过构造不同数量级别的策略属性值和不同规模的概念层次结构，本文依次分析了安全策略规则个数、规则中属性值个数、数值约束中区域个数和概念层次结构结点个数对算法运行效率的影响，从而证明算法在运行效率上是可行的。

4.期刊论文 邢昌元 改进MAC多安全策略组合方法的设计 -考试周刊2009(38)

针对支持多安全策略访问控制框架形成最终安全决定存在冲突及有效组织多个安全策略的问题,本文分析了当前主要访问控制框架的特点,提出了改进MAC多安全策略组合方法,引入了表达式匹配模式,改进了基于控制标识的安全决定策略,解决了访问控制框架在支持多安全策略时执行效率低、缺乏适应性的问题.

5.学位论文 戴怡 网格安全策略分析研究 2007

由于网格技术广泛的应用前景，网格安全正受到越来越多的关注。认证和访问控制作为网格安全的两大主要问题，引起了国内外很多政府、科研机构以及一些大型公司的重视。

本文首先介绍了网格计算技术的基本知识，包括发展历史、定义、特性、体系结构以及关键技术等。然后从安全方面着重讨论了网格的特殊性需求，并介绍了一种可扩展的网格安全体系结构，分析了现有的安全解决方案的缺陷，以及描述了目前最为成熟的网格项目Globus中的安全设施GSI(Globus Security Infrastructure)。

GSI为我们提供了单个管理域下安全认证问题的解决方案，但基于网格的广域特性，如何解决其多个域间的认证是目前亟待解决的问题。本文在讨论了现有基于身份的认证技术，特别是采用PKI(PublicKeyInfrastructure)的数字证书体系的基础上，结合网格特性，引入了“信任矩阵”的概念，根据域间映射的思想，详细阐述了单个管理域以及多个管理域间的安全认证机制。这一机制完善了网格环境中的安全认证体系。

针对网格环境下传统的基于角色的访问控制RBAC(Role-BasedAccessControl)方式中资源共享的可扩放性和欺骗问题，提出了一种动态的基于信任度的多维角色访问控制方式。这种新型的访问控制方式可以根据实体的行为动态调整它的角色，在实体的权限与它的行为之间建立了联系。

最后总结了本文提出的安全方案，并明确了未来工作方向。

6.会议论文 张红军.李亚芬 基于角色的访问控制中安全策略的应用 2001

本文基于将安全策略(Security Policy)应用于角色的访问控制(Role-Based Access Control RBAC)的思想提出了实施策略的基于角色的访问控制(Policy-Enforced Role-Based Access Control PERBAC)模型,并将公钥机制(Public Key Infrastructure PKI)和角色分配策略(Role-Assignment Policy)与PERBAC相结合提出了面向Internet应用的扩展PERBAC(Extended PERBAC EPERBAC)模型,最后设计出基于EPERBAC的访问控制系统构架.

7.学位论文 李春林 分布式访问控制安全策略的研究 2005

基于策略的管理解决方案通过策略来实现对被管理系统的分布式、自动化以及动态自适应的管理,已经成为大规模企业级网络内部分布式系统管理的最有发展前途的研究方向.本文的论题限定在分布式(异构)环境下的访问控制安全策略的研究,侧重于对分布式环境下策略冲突的研究并且提出了基于角色划分的分布式访问控制模型,通过角色的安全划分解决分布式环境下策略冲突的方法.并且实现了一个基于角色划分的分布式访问控制系统.

8.期刊论文 张展.生拥宏.祝跃飞 SE Linux安全策略灵活性研究 -信息工程大学学报2004,5(2)

安全操作系统要能够灵活充分地支持大量广泛的安全策略.这些灵活性需要支持控制访问权限的转移,执行细粒度的访问控制和撤消之前许可的访问权限.当前的一些系统在这些方面有所欠缺.本文介绍了一种操作系统安全构架可以解决当前的这些问题.构架提供了针对每个安全决策必须与安全策略做出协商的转移控制机制,使用保证安全决策一致性的安全决策缓存,并在服务组件中提供了细粒度的访问控制和撤消机制.

9.学位论文 吴新松 多安全策略访问控制的关键技术研究 2009

在网络环境中，计算机系统面临的安全威胁是复杂的、多样的和动态变化的，因而，计算机系统的安全需求具有复杂性、多样性和动态变化性等特点。研究表明，多安全策略访问控制是应对复杂、动态安全需求的有效手段。本文对多安全策略访问控制的关键技术进行了研究，并取得了以下研究成果：

第一，对操作系统的强制访问控制框架的正确性验证进行了研究，提出了正确性验证的三个目标，给出了路径敏感的基于静态分析的正确性验证方法，对TrustedBSD MAC框架进行了正确性验证，并成功发现了多处钩子函数放置错误。

第二，对RBAC模型的安全策略的动态调整进行了研究，指出了RBAC模型在安全策略动态调整，特别是角色授权动态调整方面存在的不足，给出了基于状态的安全策略动态调整模型，并给出了基于虚拟域的安全策略动态调整模型的实现方法。

第三，对RBAC模型和Clark-Wilson模型的融合进行了研究，指出了这两个模型在大型应用的完整性保护方面存在的不足，对Clark-Wilson模型的验证规则和实施规则进行了扩展，并给出了RBAC模型和Clark-Wilson模型基于层次方法的融合。

第四，对安全策略描述框架的评价进行了研究，分析了灵活表达安全策略所需的安全策略描述组件，总结了六类典型的安全策略描述框架，提出了基于描述性和实施性评价指标的安全策略描述框架的评价方法，并对六类典型的安全策略描述框架进行了评价。

本文的研究解决了多安全策略访问控制的一些关键问题，为进一步研究多安全策略的实施、多安全策略的动态调整以及多安全策略的融合等问题奠定了理论与实践基础。

10.学位论文 吴迪 分布式环境下基于角色的互操作的访问控制技术研究 2006

随着Internet及其相关技术的快速发展，在开放的、异构的分布式环境下，出现了大量的分布式应用之间的互操作，通过互操作分布式应用可以共

享资源和服务，有效的提高了数据的使用率。访问控制技术是一项关键的安全技术，它在保证合法用户访问资源的前提下，可以有效的限制用户对关键资源的访问。分布式应用所具有的分布性、异构性、自治性和动态性等特点对互操作的访问控制技术提出了许多新的挑战。

基于角色的访问控制模型(Role-Based Access Control，RBAC)是目前最为流行的访问控制技术，具有很大的灵活性。当前已经有不少研究正在探讨如何将RBAC模型应用在互操作的访问控制中，并且取得了一定的成果，但仍存在许多不足，本文对基于角色的互操作的访问控制的关键技术进行了深入的探讨和实践。本文的主要贡献如下：　　(1) 提出了一个基于角色的互操作的访问控制模型。该模型通过在不同的访问控制域之间定义角色映射关系，对RBAC模型的核心功能、继承关系和约束关系进行了全面的扩展，充分的将RBAC模型的特点应用到互操作的访问控制中。

(2) 提出了一个基于角色的互操作的分布式访问控制的体系架构。通过在原有RBAC 模型的会话基础上建立互操作的全局会话，实现了可扩展的互操作的访问控制的授权和访问检查机制。

(3) 提出了一种基于角色的互操作的安全冲突的检测算法。根据分布式环境的特点，缩小检测范围，只对参与互操作的角色进行进算，从而减少了计算所花费的时间。

(4) 提出了一个基于角色的互操作的安全策略语义规范。通过定义本体及其相关的语义规则来表达安全策略的语义信息，利用这个规范可以制定统一的互操作的安全策略，从而提高安全策略在互操作中理解的准确性。