一种基于可信等级的安全互操作模型*

谢四江[1a]，查雅行[2,1b]，池亚平[1b]

(1. 北京电子科技学院 a. 信息安全研究所；b. 通信工程系，北京 100070；2. 西安电子科技大学 通信工程学院，西安 710071)

摘　要： 传统的访问控制方式已不能满足多域环境下的资源共享和跨域访问的安全需求，建立安全互操作模型是进行安全互操作的有效途径。针对现有域间安全互操作模型未考虑用户平台的问题，提出了一种基于可信等级的域间安全互操作(TLRBAC)模型。该模型引入了用户可信等级、平台可信等级和域可信等级，制定了域间安全互操作方法。分析表明该模型既保证了用户的可信接入，又能有效地控制因平台环境而引起的安全风险问题。

关键词： 可信等级；基于角色访问控制模型；安全互操作；角色映射；域间控制

中图分类号： TP309　　**文献标志码：** A　　**文章编号：** 1001-3695(2012)05-1922-04

doi:10.3969/j.issn.1001-3695.2012.05.086

Trust level based secure interoperation model

XIE Si-jiang[1a], ZHA Ya-xing[2,1b], CHI Ya-ping[1b]

(1. *a. Information Security Institute, b. Dept. of Communication, Beijing Electronic Science & Technology Institute, Beijing* 100070, *China*; 2. *School of Telecommnunication Engineering, Xidian University, Xi'an* 710071, *China*)

Abstract: Traditional access control methods can not meet the security demand of the resource sharing and cross-domain access anymore, establishing secure interoperation model is an effective way to secure interoperation. For the neglect of the security risks caused by the user platform in the existing inter-domain interoperation security model, this paper proposed a trust level of role-based access control(TLRBAC) model. It introduced user trust level, platform trust level and domain trust level, then constituted the method of inter-domain interoperation in the model. Analysis shows that the model can not only ensure the credibility of user's access, but also effectively control the problem of security risks caused by environment of the platform.

Key words: trust level; RBAC model; secure interoperation; role mapping; inter-domain control

随着网络技术的发展，分布式环境下跨域访问和资源共享问题受到了广泛的关注，跨域安全互操作提供了一种分布式环境下的资源共享方式，传统的访问控制方式已经不能满足跨域互操作的安全需求，而确保互操作的安全性是分布式访问控制实施的关键。

为了保证互操作的安全性，域内的访问控制策略与跨域后的全局策略应该具有一致性。文献[1]中提出了针对安全互操作的指导性原则：

a)自治原则。任何自治系统中允许的操作，在建立互操作后的联合系统中也被允许。

b)安全原则。任何自治系统中禁止的操作，在建立互操作后的联合系统中也被禁止。

域间安全互操作就是在保证各个域自身安全的前提下最大程度地去实现跨域访问的安全。该原则是域间安全互操作的前提条件，为构建安全互操作模型提供了重要的参考依据。

1　相关工作

目前，国内外许多学者对 RBAC 模型[2]在自治域间安全互操作的方法进行了研究。Kapadia 等人[3]提出了基于角色映射的多域间访问控制模型 IRBAC2000，在基于角色访问控制下，尝试解决两个或多个域之间的安全互操作问题，但该模型存在诸多安全性问题。文献[4]中为建立多域环境而提出了一种安全互操作架构，在多域环境中利用使用控制(UCON)策略，并通过对属性管理辅助使用控制来保证其安全互操作。文献[5]中分析了使用 RBAC，通过对权限角色进行封装和利用最小特权原则来确保资源的安全性，并提出了有效的方案来解决角色域的发现问题，以保证多域环境下的安全互操作。文献[6]中为保证不同网格环境之间的安全互操作，在网格服务和计算系统之间实现安全互操作而引入了统一安全互操作(USI)框架，以便在执行服务调用时进行安全控制。文献[7]中通过使用约束逻辑编程，并采用 RBAC 策略保证协同环境中的安全互操作，针对互操作过程中出现的冲突问题，文中还给出了相应的解决冲突的规则。刘伟等人[8]通过引入信任度描述自治域和用户参与协作的概率，提出了一种基于信任度的自组安全互操作方法，该方法对用户和域进行信任度评估。程相然[9]提出了一种扩展的基于角色的互操作访问控制模型(EIRBAC)，给出了安全互操作实

收稿日期： 2011-10-10；**修回日期：** 2011-11-29　　**基金项目：** 国家自然科学基金资助项目(60951001)；北京市自然科学基金资助项目(4102057)；国家科技支撑计划资助项目(2009BAH52B06)；发改委信息安全产品产业化专项资助项目([2009]1886)

作者简介： 谢四江(1971-)，男，副教授，主要研究方向为信息安全(xiesj@besti.edu.cn)；查雅行(1985-)，男，硕士研究生，主要研究方向为网络安全；池亚平(1969-)，女，副教授，硕士，主要研究方向为网络安全、可信计算.

施框架和冲突的检测与消解方案,其域间授权管理的安全性和灵活性有较大提高。

上述模型的研究工作主要侧重在任务和角色上,但没有考虑用户及其所处平台环境(如软硬件平台、操作平台等)的安全状态对域间互操作的影响。而在实际中的各个域协同操作时,由于域间关系复杂,一旦存在恶意协作域、完整性受损的平台环境或恶意的用户等因素就会影响到域间互操作的安全性,为域间资源共享带来安全隐患。本文在 RBAC 模型相关研究的基础上,提出了一种基于可信等级的域间安全互操作模型(trust level of role-based access control,TLRBAC),对模型的元素及其关系进行了详细定义。模型中引入了可信等级概念并给定用户、平台和域的可信等级,制定相应角色映射规则并给出安全互操作定理。该模型既保证了用户的可信接入,又能有效地控制因平台环境因素而引起的风险。

2　TLRBAC 模型

TLRBAC 模型如图 1 所示。模型中 U、R、P、S、US、PA 和 RH 等元素的定义与 RBAC 模型[2] 中的一致,其他元素的定义如下:

a) U、R、P 和 S 分别表示用户集、角色集、权限集和会话集;$\mathrm{US}: S \to U$,表示会话集到用户集的映射函数;$\mathrm{RH} \subseteq R \times R$,表示角色集 R 上的偏序关系,如果 $\langle r_j, r_i \rangle \in \mathrm{RH}$,则角色 r_j 是角色 r_i 的父角色,继承角色 r_i 的所有权限,若角色 r_i 支配 r_j,记做 $r_i \rhd r_j$;$\mathrm{PA} \subseteq R \times P$,表示一个多对多的角色到权限的分配关系;$\mathrm{SR}: S \to 2^R$,表示会话集到角色集的幂集映射函数;$\mathrm{UA} \subseteq U \times R$,表示一个多对多的用户到角色的分配关系。

b) TL(trust-level)表示可信等级,主要描述模型中实体的可信程度,可信等级分为 trust、midtrust、lowtrust、untrust,其关系为:trust > midtrust > lowtrust > untrust。可信等级包括用户可信等级 UTL、角色可信等级 RTL、平台可信等级 PTL 和域可信等级 DTL。

c) TP 表示可信平台,是指发起访问的用户所处平台的软硬件环境属性,包括系统可信平台 $\mathrm{TP_{SYS}}$ 和应用程序可信平台 $\mathrm{TP_{APP}}$。

d) $\mathrm{UTA} \subseteq U \times \mathrm{TL}$,表示用户—可信等级分配关系,它决定了用户—角色和用户访问权限的分配。

e) $\mathrm{RTA} \subseteq R \times \mathrm{TL}$,表示角色—可信等级分配关系,系统根据给用户角色分配的可信等级,它决定了用户角色的分配。

f) $\mathrm{STA} \subseteq S \times \mathrm{TL}$,表示会话—可信等级分配关系,是一种一对多的关系,对于每个会话 S_i 只能有一个可信等级,不同的会话可以有相同的可信等级。

g) TLH(trust level hierarchy)表示可信等级层次关系,$\mathrm{TLH} \subseteq \mathrm{TL} \times \mathrm{TL}$,记做 $\leqslant_{\mathrm{tl}}$,对任意 $(L_1, L_2) \in \mathrm{TLH}$,$L_1 \leqslant_{\mathrm{tl}} L_2$ 当且仅当 $L_1 \subseteq L_2$。

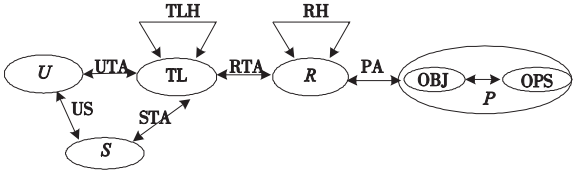

图1　TLRBAC模型

3　可信等级评估

3.1　用户可信等级评估

用户可信等级的评估主要依赖于用户在与本地安全域或外域的交互过程中获得的评价结果,用户访问完成后,由域管理员给定评价等级,等级越高可信程度越高。

对一次交互时间段 $[t_0, t_n]$ 内用户 u 在安全域 D 内以角色 r 执行 m 个事件来评估用户的可信等级,将 $[t_0, t_n]$ 分为 n 个间隔,并分别定义一个权重 w_i,用于反映每个时间间隔中用户的操作对可信等级的影响程度。通过域中策略服务器将系统事件分为:可信事件集 T、中立事件集 NT 和不可信事件集 UT。假设 E_{ik} 表示第 i 个间隔中的第 k 个事件,并给定 E_{ik} 的评估值 V_{ik},$V_{ik} \in [-1, 1]$,它表示事件的可信度。$V_{ik} \in [-1, 0)$,$E_{ik} \in UT$;$V_{ik} = 0$,$E_{ik} \in NT$;$V_{ik} \in (0, 1]$,$E_{ik} \in T$。通过对不同事件分配不同的权重值来定义不同事件的可信程度,用户与安全域之间没有直接交互时,可信度用符号 $\varnothing$ 表示,考虑到参与评估的安全域对用户的可信等级评估结果的影响不同,设影响的权重因子为 $w_j (j = 1, 2, \cdots, n)$。

在第 i 个间隔中,可信度

$$T_i = \begin{cases} \sum_{k=1}^{m} V_{ik} / \sum_{k=1}^{m} |V_{ik}| & \exists E_{ik} \in [t_{i-1}, t_i] \\ \varnothing & \text{其他} \end{cases}$$

安全域 D 对用户 u 的可信等级评估值

$$\mathrm{UTL}_u^D = \begin{cases} \sum_{j=1}^{n} w_j \times \sum_{i=1}^{m} w_i \times T_i & \exists T_i \neq \varnothing \\ \varnothing & \text{其他} \end{cases}$$

3.2　平台可信等级评估

平台可信等级是由系统根据用户访问请求时的平台信息进行确定,包括系统可信平台和应用程序可信平台,设其权重分别为 λ 和 $1 - \lambda$。考虑系统可信平台中的 n 项因素,单项权重设为 δ_i,且 $\sum_{i=1}^{n} \delta_i = 1$;考虑应用程序可信平台中的 m 项因素,其单项权重设为 μ_j,且 $\sum_{j=1}^{m} \mu_j = 1$。$\mathrm{CO_{Sys_i}}$ 和 $\mathrm{CO_{App_i}}$ 分别为实际配置系统可信平台 Sys_i 或应用程序可信平台 App_i 与各自的标准配置的对比结果,若一致,则赋值为 1,否则为 0。

采用层次分析法抽取同一层次平台影响因素中的任意两个进行比较,得出在特定环境下执行某一事件时的权重关系,并将其量化为判断矩阵,得到系统可信平台判断矩阵 $\boldsymbol{A} = (a_{ij})_{n \times n}$ 和应用可信平台的判断矩阵 $\boldsymbol{B} = (b_{ij})_{m \times m}$,并计算出系统可信平台和应用可信平台各指标的权重值,方法如下:

$$\delta_i = \frac{1}{n} \sum_{j=1}^{n} \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} \quad i = 1, 2, \cdots, n$$

$$\mu_i = \frac{1}{n} \sum_{j=1}^{m} \frac{b_{ij}}{\sum_{k=1}^{m} b_{kj}} \quad i = 1, 2, \cdots, m$$

经计算得出系统可信平台和应用程序可信平台各指标的权重值,最终得到平台可信等级评估值 $\mathrm{PTL_{TP}}$:

$$\mathrm{PTL_{TP}} = \lambda \times \sum_{i=1}^{n} \delta_i \mathrm{CO_{Sys_i}} + (1 - \lambda) \times \sum_{j=1}^{m} \mu_j \mathrm{CO_{App_i}}$$

3.3　安全域可信等级评估

在用户跨安全域访问的时候,为避免恶意域的非法操作,

保证域间互操作的安全性,需要考虑安全域的可信程度。域间的信任关系也是影响安全互操作的重要因素,安全域可信等级评估值主要是安全域之间信任评估的结果。域之间的信任评估是动态变化的,它是由本域用户、外域用户给定的信任评估结果以及外域历史信任评估结果决定的。

假设有 N 个安全域,N 中第 j 个安全域 D_j 有 m_j 个用户,安全域 D_i 有 m_i 个用户。$U_{D_j}^{i}$ 表示域 D_j 中第 $i(1<i\leqslant m_j)$ 个用户;域信任度函数 $\text{trust}(D_j,D_i)$ 表示域 D_j 对域 D_i 的信任程度,$\text{trust}(D_j,D_i)\in(0,1]$;$\text{trust}(D_j,D_i)^M$ 表示域 D_j 对域 D_i 的第 M 次访问事件后 D_i 获得 D_j 的信任程度,即 D_i 最终获得的可信等级评估值。由于不同域的用户对同一域进行信任评估的考虑因素不一样,为保证评估结果的合理性,设置权重值 w_1、w_2 和 w_3,$w_1+w_2+w_3=1$,具体使用如下公式。因此,在跨域访问的第 M 次访问事件后,域 D_i 获得的可信等级评估结果可由下式计算得到:

$$\text{DTL}_D=\text{trust}(D_j,D_i)^M=w_1\times\frac{\sum_{j=1,j\neq i}^{N}\sum_{i=1}^{m}\text{trust}(U_{D_j}^{i},D_i)^M}{m\times N}+$$

$$w_2\times\frac{\sum_{i=1}^{n}\text{trust}(U_{D_i}^{i},D_i)^M}{n}+w_3\times\sum_{j=1,j\neq i}^{N}\text{trust}(D_j,D_i)^{M-1}$$

其中:w_1 表示外域用户对域 D_i 的信任评估结果的权重;w_2 表示本域用户对域 D_i 的信任评估结果的权重;w_3 表示外域对域 D_i 的历史信任评估结果的权重。

3.4 可信等级评估值

由 UTL、PTL 和 DTL 确定用户在访问目标域前的可信等级评估值 TLE,并给出与可信等级的关系,以便用户在进行跨域访问时,目标域可以利用可信等级的值作出更直接的判断。TLE 可以表示如下:

$$\text{TLE}=\begin{cases}w_u\times\text{UTL}_u^D+w_{\text{tp}}\times\text{PTL}_{\text{TP}}+w_d\times\text{DTL}_D & T_i\notin\varnothing\\ \varnothing & \text{其他}\end{cases}$$

其中:w_u 表示用户可信等级的权重;w_{tp} 表示用户平台可信等级的权重;w_d 表示用户所在域的可信等级权重。$w_u,w_{\text{tp}},w_d\in[0,1]$,且 $w_u+w_{\text{tp}}+w_d=1$。则 $\text{TLE}\in[0,1]$,TLE 的值越大表示可信等级越高,TLE 与 TL 之间的关系如下:

$$\text{TL}=\begin{cases}\text{trust} & \text{TLE}\in[0.9,1]\\ \text{midtrust} & \text{TLE}\in[0.75,0.9)\\ \text{lowtrust} & \text{TLE}\in[0.6,0.75)\\ \text{untrust} & \text{TLE}\in[0,0.6)\end{cases}$$

4 TLRBAC 模型规则

假设多域环境中自治域构成的集合 $D=\{D_1,D_2,\cdots,D_n\}$,设 D_i 和 D_j 分别为本地域和外域,将外域 D_j 角色集 R_j 中角色 r_i 与本地域 D_i 角色集 R_i 中角色 r_j 建立角色映射的关联记做 $r_j\mapsto r_i$ 或(r_j,r_i),设 r_j 的父角色和子角色分别为 r_{fj}和 r_{jc},r_i 的父角色和子角色分别为 r_{fi}和 r_{ic}。用户在访问请求时用户和平台要满足系统要求的可信等级阈值分别为 UTL^* 和 PTL^*。

1)角色关系性质

a) $\forall r_1、r_2、r_u,r_1\geqslant r_2\wedge r_1\in r_u\Rightarrow r_2\in r_u$。

b) $\forall r_y\in R_j,r_j\geqslant r_y\wedge\langle r_{fj},r_j\rangle\Rightarrow\langle r_{fj},r_y\rangle$;$r_y\geqslant r_j\wedge\langle r_j,r_{jc}\rangle\Rightarrow\langle r_y,r_{jc}\rangle$。

c) $\forall r_x\in R_i,r_i\geqslant r_x\wedge\langle r_{fi},r_i\rangle\Rightarrow\langle r_{fi},r_x\rangle$;$r_x\geqslant r_i\wedge\langle r_i,r_{ic}\rangle\Rightarrow\langle r_x,r_{jc}\rangle$。

2)默认映射(default mapping,DM)规则 $\forall r_x\in R_i,r_y\in R_j,r_j\geqslant r_y\wedge r_i\geqslant r_x\wedge\langle r_j,r_i\rangle\wedge\langle r_j,r_x\rangle\wedge\langle r_{fj},r_i\rangle\wedge\langle r_{fj},r_x\rangle\Leftrightarrow r_j\mapsto_{\text{DM}} r_i$。

3)显式映射(explicit mapping,EM)规则 $\forall r_x\in R_i,r_y\in R_j,r_j\geqslant r_y\wedge r_i\geqslant r_x\wedge\langle r_j,r_i\rangle\wedge\langle r_j,r_x\rangle\Leftrightarrow r_j\mapsto_{\text{EM}} r_i$。

4)隐式映射(implicit mapping,IM)规则 $\forall r_x\in R_i,r_y\in R_j,r_j\geqslant r_y\wedge r_i\geqslant r_x\wedge\langle r_j,r_i\rangle\wedge\langle r_{fj},r_i\rangle\wedge\langle r_{fj},r_x\rangle\Leftrightarrow r_j\mapsto_{\text{IM}} r_i$。

5)拒绝映射(refuse mapping,RM)规则 $\forall r_x\in R_i,r_y\in R_j,r_j\geqslant r_y\wedge r_i\geqslant r_x\wedge\langle r_j,r_i\rangle\notin\text{RM}\wedge r_j\trianglerighteq r_i\wedge r_j\trianglelefteq r_i\Leftrightarrow r_j\mapsto_{\text{RM}} r_i$。

6)可信等级阈值(trust level threshold,TLT)规则 $\forall u\in U,r_i\in R_i,r_j\in R_j,\text{UTL}_u\leqslant\text{UTL}^*\vee\text{PTL}_u\leqslant\text{PTL}^*\vee\text{TL}=\text{untrust}\Rightarrow(r_i,r_j)\in\text{RM}$。

7)互操作定理 由 $D_i=\langle U_i,R_i,P_i,\text{TL}_i,\text{RH}_i,\text{TLH}_i,\text{UTA}_i,\text{RTA}_i,\text{PA}_i\rangle(i=1,2,\cdots,n)$ 构成的多自治域环境,互操作 $I=\langle\cup_1^n D_i,S,\text{TLT},\text{DM},\text{EM},\text{IM},\text{RM}\rangle$ 是安全的,当且仅当满足:

S_1: $\forall r_1\in R_i,r_2\in R_i,r_1\rhd r_2\Rightarrow r_1\geqslant r_2$

S_2: $\forall r_i\in R_i,r_j\in R_j,r_i\rhd r_j\wedge i\neq j\Rightarrow(r_i,r_j)\notin\text{RM}$

S_3: $\forall u\in U_i,r_i\in R_i,r_j\in R_j,\text{UTL}_u>\text{UTL}^*\vee\text{PTL}_u>\text{PTL}^*\vee\text{TL}\neq\text{untrust}\Rightarrow(r_i,r_j)\notin\text{RM}$

5 TLRBAC 模型安全性分析

对 TLRBAC 模型进行安全性分析主要是对互操作定理进行分析和证明,其互操作定理是在进行域间互操作时判定是否满足安全性原则的条件。当使用 TLRBAC 模型进行域间互操作时,可以根据该定理进行判断,若满足定理,则互操作是安全的。

根据域间安全互操作的指导性原则,本模型在进行域间互操作时具备以下安全特性:角色层次关系不会因域间互操作而改变;域间角色映射生成的角色层次关系不符合自治域定义的拒绝映射规则;域间角色映射不能违反可信等级阈值规则。互操作 I 是安全的,当且仅当 I 能同时满足约束条件 S_1、S_2 和 S_3,证明如下:

证明

1)充分性 TLRBAC 模型的域间互操作 I 满足约束条件 S_1、S_2 和 S_3,则 I 是安全的。

a)I 满足 S_1,即 $r_1\rhd r_2\Rightarrow r_1\geqslant r_2$。因为对 $\forall r_1,r_2\in R_i$,若 $r_1\ngeqslant r_2$,明显有 $r_1\not\trianglerighteq r_2$,即逆否命题成立,可知角色层次关系不会因域间互操作而改变,S_1 成立。

b)I 满足 S_2,即 $r_i\in R_i,r_j\in R_j,r_1\rhd r_2\wedge i\neq j\Rightarrow(r_i,r_j)\notin\text{RM}$。因为其逆否命题明显成立,即对 $r_i\in R_i,r_j\in R_j,((r_i,r_j)\in\text{RM})\wedge i\neq j\Rightarrow r_i\not\trianglerighteq r_j$,即可知域间角色映射后,角色的支配关系不符合自治域定义的拒绝映射规则,S_2 成立。

c)I 满足 S_3,即 $\forall u\in U,r_i\in R_i,r_j\in R_j,\text{UTL}_u>\text{UTL}^*\vee\text{PTL}_u>\text{PTL}^*\vee\text{TL}\neq\text{untrust}\Rightarrow(r_i,r_j)\notin\text{RM}$。因为对 $\forall u\in U,r_i\in R_i,r_j\in R_j,(r_i,r_j)\in\text{RM}$,由 RM、$\text{UTL}^*$、$\text{PTL}^*$ 和 TL 的定义可知,$\text{UTL}_u\leqslant\text{UTL}^*\vee\text{PTL}_u\leqslant\text{PTL}^*\vee\text{TL}=\text{untrust}$,其逆否命题成立,

S_3 成立。充分性成立。

2)必要性　若 TLRBAC 模型的域间互操作 I 是安全的,则约束条件 S_1、S_2 和 S_3 都成立。

a)根据角色层次关系的定义可知,对于 $\forall r_1, r_2 \in R_i$,在互操作过程中,若 $r_1 \triangleright r_2$,则在域内有 r_2 继承 r_1,$r_1 \geqslant r_2$,即 S_1 成立。

b)互操作 I 是安全,根据域间互操作的安全原则,在单域中禁止的操作在互操作中也禁止,对 $\forall r_i \in R_i, r_j \in R_j, r_i \triangleright r_j \wedge i \neq j$,角色映射后生成的角色支配关系 (r_i, r_j) 不能违反拒绝映射规则 $(r_i, r_j) \notin \mathrm{RM}$,即 S_2 成立。

c)根据域间角色映射不能违反可信等级阈值规则,$\forall u \in U, r_i \in R_i, r_j \in R_j$,若 $(r_i, r_j) \in \mathrm{RM}$,则 $\mathrm{UTL}_u > \mathrm{UTL}^*$ 或 $\mathrm{PTL}_u > \mathrm{PTL}^*$ 或 $\mathrm{TL} \neq \mathrm{untrust}$,逆否命题成立,即 S_3 成立。必要性成立。

通过证明分析,在 TLRBAC 模型基础上的互操作 I 是安全的。

6　结束语

本文通过引入可信等级来构建一种新的安全互操作模型,在该模型的基础上制定了角色映射的规则和互操作的安全性判定定理,并给出了模型的安全性分析与证明。在进行域间安全互操作时,可依据安全互操作定理来保证域间互操作的安全性,下一步工作主要是在使用该模型进行跨域访问时,对角色映射带来的冲突检测与消解以及对资源的跨域访问等问题进行深入的研究。

参考文献:

[1] LI Gong, QIAN Xiao-lei. The complexity and composability of secure interoperation[C]//Proc of IEEE Computer Society Symposium on Research in Security and Privacy. Washington DC: IEEE Computer Society, 1994: 190-200.

[2] FERRAIOLO D F, SANDHU R, GAVRILA S, *et al*. Proposed NIST standard for role-based access control[J]. ACM Trans on Information and System Security, 2001, 4(3): 224-274.

[3] KAPADIA A, AL-MUHTADI J, CAMPBELL R H, *et al*. IRBAC 2000: secure interoperability using dynamic role translation, UIUC-DCS-R-2000-2126[R]. Champaign, IL: University of Illinois, 2000.

[4] ZHAO Guang, LU Jun-li, YANG Fan, *et al*. A usage-based authorization architecture for multidomain environments[C]//Proc of the 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing. 2010: 245-248.

[5] ZHANG Yue, JOSHI J B D. Role-based domain discovery in decentralized secure interoperations[C]//Proc of International Symposium on Collaborative Technologies and Systems. 2010: 84-93.

[6] LIU Guo-hua. USI-Uniform secure interoperation in grid service and computing system[C]//Proc of 2nd International Conference on Information Engineering and Computer Science, 2010: 1-4.

[7] HU Jin-wei, LI Rui-xuan, LU Zheng-ding. RBAC-based secure interoperation using constraint logic programming[C]//Proc of the International Conference on Computational Science and Engineering. 2009: 867-872.

[8] 刘伟,蔡嘉勇,贺也平. 一种基于信任度的自组安全互操作方法[J]. 软件学报, 2007, 18(8): 1958-1967.

[9] 程相然. 多域环境下基于角色的安全互操作关键技术研究[D]. 郑州:解放军信息工程大学, 2010.

[10] 金莉,卢正鼎,赵峰. 多域环境下安全互操作研究进展[J]. 计算机科学, 2009, 36(2): 47-54.

[11] 王雅哲,冯登国. 域间授权互操作研究综述[J]. 计算机研究与发展, 2010, 47(10): 1673-1689.