2010年 11月 北京航空航天大学学报 November 2010
第36卷 第11期 Journal of Beijing University of Aeronautics and Astronautics Vol. 36 No. 11

基于描述逻辑 DL_{RBAC} 的 RBAC 形式化模型

马 丽 马世龙 眭跃飞

(北京航空航天大学 计算机学院，北京 100191) (中国科学院 计算技术研究所，北京 100190)

摘 要：提出了一种新的基于描述逻辑的形式化表示方法，将组成基于角色的访问控制(RBAC，Role-Based Access Control)模型的集合和关系分别用描述逻辑中的概念和角色表示，并且在基本的描述逻辑语言上引入了可以表示角色的复合关系和包含关系的符号，从而形式化表示出了RBAC与角色继承有关的一些关键性质和约束条件，如角色层次关系(RH，Role Hierarchy)传递性、用户角色分配关系(UA，User-Role Assignment)的继承性和权限角色分配关系(PA，Permission-Role Assignment)的继承性，以及RBAC中的静态职权分离约束和动态职权分离约束等.通过形式化地表示RBAC的继承关系及约束条件，利用描述逻辑本身的推理机制可以限制不符合访问控制策略的继承关系产生.

关 键 词：访问控制；基于角色的访问控制；描述逻辑

中图分类号：TP 309

文献标识码：A **文 章 编 号**：1001-5965(2010)11-1315-05

Representation for RBAC model with description logic DL_{RBAC}

Ma Li Ma Shilong

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Sui Yuefei

(Information Processing Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: A new description logic-based representation for role-based accesss control(RBAC) model was proposed. RBAC sets and relations were translated as concepts and roles in the description logic respectively. To express RBAC role default inheritance and constraint conditions, symbols that represented role composition and inclusion were introduced to the basic description logic language, such that some RBAC default inheritance properties, such as role hierarchy(RH) transitivity, user-role assignment(UA) inheritance and permission-role assignment(PA) inheritance, and some RBAC constraints, such as static and dynamic separation of duty relations, can be represented formally. By integrating default inheritance with constraints in one formal system, the new inheritance relations that violate the access control strategy can be limited with the help of description logic reasoning mechanisms.

Key words: access control model; role-based access control model; description logic

在开放的、动态的环境中，应用变得越来越复杂及智能化，需要更高程度的决策和自治，例如Grid计算、Web服务和普适计算等.为这种应用提供安全保障是当前的一个挑战[1].基于角色的访问控制(RBAC，Role-Based Access Control)通过角色来控制对资源的访问[2-3]，由于具有“策略中立”和管理简单等特性，它一直被认为是能适应动态环境应用的访问控制模型[4-5].

随着语义Web技术的出现，对访问控制策略的描述也需要适应跨领域、异构的环境，以促进不同应用环境的参与者之间的相互理解.在这种情况下，为了提供一种形式的、可共享的访问控制规范语言，用基于语义Web的语言来表示RBAC模型已经得到越来越多的重视，如Web本体语言(OWL，Web Ontology Language)[1,6].描述逻辑(DL，Discription Logic)[7]作为OWL的形式化基础[8]，对开发能适应Web环境的访问控制语言具有积极的意义.

收稿日期：2009-10-12

基金项目：国家973重点基础研究发展规划资助项目(2005CB321902)

作者简介：马 丽(1974－)，女，安徽安庆人，博士生，mali@nlsde.buaa.edu.cn.

目前已有一些用描述逻辑对RBAC模型进行形式化描述的研究[9-11],但这些表示方法存在一些问题.例如文献[9]用描述逻辑语言对RBAC 96模型进行形式化表示,其中将角色作为概念,将角色层次表示为不同角色概念之间的包含关系,然而这种方法找不到合理的语义解释,且无法将RBAC中的角色继承关系表示出来.而文献[10-11]提出的描述逻辑方法与文献[9]有类似的表示,并没有解决这个问题.除此之外,已有的RBAC描述逻辑表示方法只能表达简单的用户与角色、角色与权限的直接关系,但如果要表达用户与权限之间的通过角色构建的复合关系,在表示能力上不够.

出于以上原因,本文将结合RBAC 96模型和描述逻辑语言,提出一种新的RBAC描述逻辑表示方法,补充RBAC模型中的继承性定义及语义解释.

1 RBAC模型的描述逻辑 DL_{RBAC}

RBAC 96模型[2]将传统的RBAC模型根据不同需要拆分成4种嵌套的子模型:基本模型$RBAC_0$,角色层次模型$RBAC_1$,约束模型$RBAC_2$和整体模型$RBAC_3$.本节先简单介绍一下描述逻辑基础,然后提出RBAC的描述逻辑表示,并分别用DL_0,DL_1和DL_2表示$RBAC_0$,$RBAC_1$和$RBAC_2$的描述逻辑,而DL_{RBAC}则为这些描述逻辑的总称.

1.1 描述逻辑基础

基本的描述逻辑语言ALC(Attributive Language with Complement)[8]包含如下基本符号:个体常元a_0,a_1,…;原子概念名A_0,A_1,…;概念名C_0,C_1,…;角色R_0,R_1,…;顶概念$\top$,底概念$\bot$;概念构造子$\neg$,$\sqcap$,$\exists$;断言构造子$\sqsubseteq$;逻辑连接词:$\rightarrow$,$\neg$.

定义1 概念C定义如下:

$$C::=A \mid \top \mid \bot \mid \neg C \mid C_1 \sqcap C_2 \mid \exists R.C$$

定义2 断言φ定义如下:

$$\varphi::=C(a) \mid R(a,b) \mid C_1 \sqsubseteq C_2 \mid \neg \varphi \mid \varphi_1 \rightarrow \varphi_2$$

其中,C为概念;R为角色;a,b为个体常元.

定义3 在一定领域中,一个知识库KB=(TBox,ABox)由两个部分组成,其中TBox是一个关于包含断言的有限集合,也称为术语公理的集合;ABox是概念断言和角色断言的有限集合.

术语公理有包含($\sqsubseteq$)公理和相等($\equiv$)公理.

ALC语义将概念解释为一个非空的论域的子集,角色是该论域上的二元关系.形式上,一个解释$I=(\Delta^I,\cdot^I)$由一个非空集合Δ^I和一个解释函数$\cdot^I$组成,使得对每个原子概念A,$A^I\subseteq\Delta^I$,对每个原子角色R,$R^I\subseteq\Delta^I\times\Delta^I$.

定义4 断言φ在解释I中为真,记为$I\models\varphi$,如果满足如下条件:

1) $C^I\subseteq D^I$,如果$\varphi=C\sqsubseteq D$;

2) $a^I\in C^I$,如果$\varphi=C(a)$;

3) $(a^I,b^I)\in R^I$,如果$\varphi=R(a,b)$;

4) $I\not\models\psi$,如果$\varphi=\neg\psi$,其中ψ为断言;

5) $I\models\psi_1\Rightarrow I\models\psi_2$,如果$\varphi=\psi_1\rightarrow\psi_2$,其中$\psi_1$和$\psi_2$为断言.

本文将在ALC基础上提出RBAC的描述逻辑.

1.2 $RBAC_0$的描述逻辑

$RBAC_0$的模型S_0为一个九元组(U,*Role*,P,S,UA,PA,*user*,*roles*,*permissions*).其中:U为用户的集合;*Role*为一般角色的集合;P为一般权限的集合;S为会话的集合;$UA\subseteq U\times Role$,为用户到角色的分配关系;$PA\subseteq P\times Role$,为权限到角色的分配关系;*user*,*roles*和*permissions*为函数,满足:$user:S\rightarrow U$将每个会话s映射为一个用户(不会改变);$roles:S\rightarrow 2^{Role}$将每个会话s映射为集合$roles(s)\subseteq\{r:(user(s),r)\in UA\}$;$permissions:S\rightarrow 2^P$,每个会话s有权限$permissions(s)=\bigcup_{r\in roles(s)}\{p:(p,r)\in PA\}$.

$RBAC_0$的描述逻辑DL_0的语言L_0包含如下符号:用户的个体常量名u_0,u_1,…;角色的个体常量名r_0,r_1,…;权限的个体常量名p_0,p_1,…;会话的个体常量名s_0,s_1,…;原子概念名U,R,P,S;原子角色名UA,PA,user,roles,permissions;概念构造子$\neg$,$\sqcap$,$\exists$;角色构造子$^-$,$\circ$;包含关系$\sqsubseteq$.

定义5 概念C定义为

$$C::=U \mid R \mid P \mid S \mid \neg C \mid C\sqcap D \mid \exists R.C$$

其中,R为角色,定义为

$$R::=UA \mid PA \mid user \mid roles \mid permissions \mid R^- \mid \sim R \mid R_1\circ R_2$$

其中,$\sim R$表示R的否定形式;$R_1\circ R_2$表示R_1和R_2的复合.

定义6 断言φ定义为

$$\varphi::=U(u) \mid R(r) \mid P(p) \mid S(s) \mid UA(u,r) \mid PA(p,r) \mid user(s,u) \mid roles(s,r) \mid permissions(s,p) \mid C(c) \mid R(c,d) \mid \neg\varphi \mid \varphi\rightarrow\psi$$

其中,c,d 为常量符号.

DL_0 包含如下公理:

公理 1　$\exists PA.R \sqsubseteq P$;

公理 2　$\exists UA.R \sqsubseteq U$;

公理 3　$\exists userU.\sqsubseteq S$;

公理 4　$\exists roles.R \sqsubseteq S$;

公理 5　$\exists permissions.P \sqsubseteq S$.

定义 7　$RBAC_0$ 的模型 $M_0=(\Delta, I)$,其中:Δ 为非空集合;I 为解释,使得对任意的常量符号 c,$c^I \in \Delta$;对任意的原子概念 $C, C^I \subseteq \Delta$;对任意的原子角色 $r, r^I \subseteq \Delta^2$,且 U^I, R^I, P^I 和 S^I 两两不相交;$UA^I \subseteq U^I \times R^I$; $PA^I \subseteq P^I \times R^I$; $user^I, roles^I, permissions^I$ 为函数,$user^I \subseteq S^I \times U^I$, $roles^I \subseteq S^I \times R^I$, $permissions^I \subseteq S^I \times P^I$.

定义 8　断言 φ 在模型 M_0 中是可满足的,如果 $M_0 \models \varphi$;φ 为可满足的,如果 φ 在每个模型 M_0 中都是可满足的.

命题 1　公理 1～5 在 M_0 中都是可满足的.

定义 9　permissions 的可定义性指的是 permissions 可以用其他的原子角色定义.

命题 2　permissions 在 ALC 中是不可定义的.

permissions 在 L_0 中可以用 roles 和 PA 定义,表示如下:

公理 6　$permissions = \sim(roles \circ \sim PA^-)$.

公理 6 称为权限激活公理.

对任意会话 $s \in S$ 所满足的条件 $roles(s) \subseteq \{r : (user(s), r) \in UA\}$ 可以表示如下:

公理 7　$roles \sqsubseteq \sim(user \circ \sim UA)$.

为了使公理 6 和公理 7 在 $RBAC_0$ 的模型 M_0 中有效,要求 M_0 满足如下条件:对任意 s,$roles^I(s^I) \subseteq \{r \in R^I : (user^I(s^I), r) \in UA^I\}$;对任意 s,$permissions^I(s^I) = \bigcup_{r \in roles^I(s^I)} \{p \in P^I : (p, r) \in PA^I\}$.

定义 10　DL_0 的知识库 $KB_0=(TBox_0, ABox_0)$,其中:$TBox_0$ 包含公理 1～7; $ABox_0$ 包含断言 φ(见定义 6).

1.3　$RBAC_1$ 的描述逻辑

$RBAC_1$ 的模型 S_1 为十元组 $(U, Role, P, S, UA, PA, RH, user, roles, permissions)$,其中 $RH \subseteq Role \times Role$ 为 $Role$ 上的偏序(也可用 $\leqslant$ 表示);对任意 $s \in S$, $roles(s) \subseteq \{r : \exists r' \geqslant r((user(s), r') \in UA)\}$;对任意 $s \in S$, $permissions(s) = \{p : \forall r \in roles(s)\ \exists r' \leqslant r((p, r') \in PA)\}$.

DL_1 的语言 L_1 除了包含 L_0 的所有符号,还包含原子角色:RH.

DL_1 除了包含 DL_0 中的公理 1～7 外,还包含如下公理:

公理 8　$\exists RH.R \sqsubseteq R$;

公理 9　$\exists RH.\top \equiv \exists RH.R$.

定义 11　$RBAC_1$ 的模型 M_1 为序对 (Δ, I),也是 $RBAC_0$ 的模型,且还要满足如下的条件:$RH^I \subseteq R^I \times R^I$ 为 R 偏序关系;UA^I 为 RH^I 下的闭包,即,对任意 $u \in U^I$, $r, r' \in R^I$,如果 $(u, r) \in UA^I$ 且 $(r, r') \in RH^I$,则 $(u, r') \in UA^I$.

命题 3　对满足定义 11 的模型 M_1,公理 1～9 在 M_1 中都是有效的.

此外还有如下公理:

公理 10　$\exists RH.(\exists RH.R) \sqsubseteq \exists RH.R$;

公理 11　$\exists RH.(\exists UA^-.U) \sqsubseteq \exists UA^-.U$.

命题 4　M_1 满足公理 10.

证明　在模型 M_1 中有 $RH = RH^I$, $Role = R^I$,则

$$r \in (\exists RH.(\exists RH.R))^I \Leftrightarrow$$
$$r \in \{r \mid \exists r'((r, r') \in RH \,\&\, r' \in (\exists RH.R)^I)\} \Leftrightarrow$$
$$r \in \{r \mid \exists r'((r, r') \in RH \,\&\, (\exists r''((r, r'') \in RH \,\&\, r'' \in Role)))\} \Leftrightarrow$$
$$r \in \{r \mid \exists r' \exists r''((r, r') \in RH \,\&\, (r', r'') \in RH \,\&\, r'' \in Role)\}$$

显然 $\{r \mid \exists r' \exists r''((r, r') \in RH \,\&\, (r', r'') \in RH \,\&\, r'' \in Role)\} \subseteq \{r \mid \exists r'((r, r') \in RH \,\&\, r' \in Role\}$,也就是对模型 M_1,有 $(\exists RH.(\exists RH.R))^I \subseteq (\exists RH.R)^I$,即 $M_1 \models \exists RH.(\exists RH.R) \sqsubseteq \exists RH.R$.　**证毕**

公理 10 称为 RH 的传递性.

命题 5　$M_1 \models \exists RH.(\exists UA^-.U) \sqsubseteq \exists UA^-.U$,即 M_1 满足公理 11.

证明　在模型 M_1 中,有 $UA = UA^I$, $U = U^I$, $RH = RH^I$,则

$$r \in (\exists RH.(\exists UA^-.U))^I \Leftrightarrow$$
$$r \in \{r \mid \exists r'((r, r') \in RH \,\&\, r' \in (\exists UA^-.U)^I)\} \Leftrightarrow$$
$$r \in \{r \mid \exists r'((r, r') \in RH \,\&\, (\exists u((r', u) \in I(UA^-) \,\&\, u \in U)))\} \Leftrightarrow$$
$$r \in \{r \mid \exists r' \exists (u(r, r') \in RH \,\&\, (u, r') \in UA \,\&\, u \in U)\}$$

显然 $\{r \mid \exists r' \exists u((r, r') \in RH \,\&\, (u, r') \in UA \,\&\, u \in U)\} \subseteq \{r \mid \exists u((r, u) \in (UA^-)^I \,\&\, u \in U)\}$,由此可知 $r \in \{r \mid \exists u((r, u) \in (UA^-)^I \,\&$

$u\in U)\}$，所以有 $(\exists RH.(\exists UA^{-}.U))^{I}\subseteq(\exists UA^{-}.U)^{I}$，即 $M_1\models\exists RH.(\exists UA^{-}.U)\sqsubseteq\exists UA^{-}.U$. **证毕**

公理11也称为UA-继承性，可以表示为 $UA\circ RH\sqsubseteq UA$.

条件：对任意 $s\in S$，$roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\}$ 可以表示为

公理12 $roles\sqsubseteq(\sim(user\circ\sim UA))\circ RH^{-}$.

此外还有描述PA-继承性(即，低角色的权限可以被高角色的权限包含)的公理13：

公理13 $\exists RH^{-}.(\exists PA^{-}.P)\sqsubseteq\exists PA^{-}.P$.

命题6 M_1 满足公理13.

证明 在 M_1 中 $RH=RH^{I}$，$PA=PA^{I}$，$P=P^{I}$，则

$$r\in(\exists RH^{-}.(\exists PA^{-}.P))^{I}\Leftrightarrow$$
$$r\in\{r|\exists r'((r',r)\in RH\ \&\ r'\in(\exists PA^{-}.P)^{I})\}\Leftrightarrow$$
$$r\in\{r|\exists r'((r',r)\in RH\ \&$$
$$\exists p((p,r')\in PA\ \&\ p\in P))\}\Leftrightarrow$$
$$r\in\{r|\exists r'\exists p((r',r)\in RH\ \&$$
$$(p,r')\in PA\ \&\ p\in P)\}$$

显然 $r\in\{r|\exists p((p,r)\in PA\ \&\ p\in P)\}$，这样 $(\exists RH^{-}.(\exists PA^{-}.P))^{I}\subseteq(\exists PA^{-}.P)^{I}$，即 $\exists RH^{-}.(\exists PA^{-}.P)\sqsubseteq\exists PA^{-}.P$ 在 M_1 中满足.

证毕

对 *permissions* 所满足的条件 $permissions(s)=\{p:\forall r\in roles(s)\exists r'\leqslant r((p,r')\in PA)\}$ 可以用公理的形式表示如下：

公理14 $permissions=\sim(roles\circ\sim(RH^{-}\circ PA^{-}))$，称为加入了角色层次的权限激活公理.

1.4 $RBAC_2$ 的描述逻辑

$RBAC_2$ 的模型 S_2 为十元组 $(U,Role,P,S,UA,PA,user,roles,permissions,\Delta')$，其中 Δ' 为约束的集合.

本文只讨论角色互斥约束.

接下来只考虑对UA的职能分离约束. 对任何 $r_1,r_2\in Role$，如果 r_1 和 r_2 为互斥角色关系，用 *mutex* 表示，即 $(r_1,r_2)\in mutex$.

$RBAC_2$ 的描述逻辑 DL_2 语言 L_2 除了包含 L_0 所有符号，还包含原子角色 mutex；

DL_2 除了包含 DL_0 的公理1～7外，还包含公理15：

公理15 $\exists mutex.R\sqsubseteq R$.

互斥角色约束可用于静态职能分离和动态职能分离，为了表示这一点，对任意的 u，s，角色mutex还满足公理16和公理17.

公理16 $\exists UA^{-}.u\sqcap\exists mutex.(\exists UA^{-}.u)\equiv\perp$.

公理17 $\exists roles^{-}.s\sqcap\exists mutex.(\exists roles^{-}.s)\equiv\perp$.

定义12 $RBAC_2$ 的模型 M_2 为序对 (Δ,I)，也是 $RBAC_0$ 的模型，且还要满足如下的条件：$mutex^{I}\subseteq R^{I}\times R^{I}$，且 $mutex^{I}$ 满足：对任意 $r_1,r_2\in R^{I}$，如果 $(r_1,r_2)\in mutex^{I}$，则根据静态职能分离约束，对任意 $u\in U^{I}$，如果 $(u,r_1)\in UA^{I}$，则 $(u,r_2)\notin UA^{I}$. 对动态职能分离约束，对任意 $s\in S^{I}$，如果 $(user(s),r_1)\in roles^{I}$，则 $(user(s),r_2)\notin roles^{I}$.

命题7 模型 M_2 满足公理15～17.

有了 $RBAC_1$ 和 $RBAC_2$ 模型，可以将角色层次和约束放在一个模型来表示，即 $RBAC_3$. 这里不再详细描述.

2 相关比较

目前已有的基于描述逻辑的RBAC模型有文献[9]提出的在RBAC 96模型基础上的形式化表示，也有其他的基于描述逻辑的方法都是在此表示基础上的扩充，其中对概念和角色的表示及激活和权限分配等关系上与本文的方法有所不同. 为了说明它们的不同点，本文重点与文献[9]的形式化表示进行比较. 主要有以下不同：

1) 文献[9]的表示方法没有对角色层次RH表示，直接利用子概念 RR_1 和 RR_2 之间的包含关系来表示它们实例之间的优势关系，即 $RR_1\sqsubseteq RR_2$. 这样做显然存在缺陷，首先找不到语义模型解释这种关系；其次，对RBAC模型中隐含的角色继承无法表示；

2) 对用户和权限的关系，文献[9]的描述逻辑方法定义了用户和权限之间的直接关系 authorize，并用授权公理：$\exists assign.(\exists cando.P)\sqsubseteq\exists authorize.P$ 表示了用户间接获取权限的关系，但这种表示在RBAC中是没有定义的，所以还需要将 authorize 另外定义为 assign 和 cando 的复合形式，即 $authorize=assign\circ cando$. 由于缺乏表示角色复合的符号“∘”，已有的描述逻辑方法表示能力不够.

此外，文献[9]的表示全部只是语法的形式，没有语义解释，所以很难判断表示是否合理.

3 实例分析

用文献[9]的例子来说明本文的描述逻辑表

示与文献[9]的不同,这里增加了互斥角色.

在软件开发部门有 4 种角色: Supervisor, TestEngineer, Programmer, Member, 及 3 种权限: Execute, WriteSrc, ReadDocs. 角色层次如图 1 所示. Supervisor 高于 TestEngineer 和 Programmer, 后两者又高于 Member. 假设 TestEngineer 拥有执行项目的权限, Programmer 有权限写源代码, Member 只能读文档. TestEngineer 和 Programmer 为互斥角色.

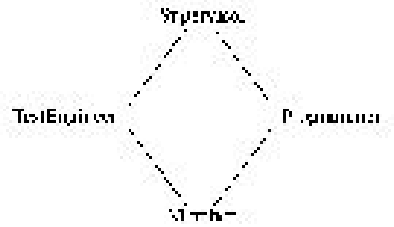

图 1　软件开发部门的角色层次图

描述 RBAC 的知识库 $KB=(TBox, ABox)$, 其中 $TBox$ 包含了第 1 节中的公理,这里不再重复, $ABox$ 则包含如下初始断言:

{R(Supervisor), R(TestEngineer), R(Programmer), R(Member), RH(TestEngineer, Supervisor), RH(Programmer, Supervisor), RH(Member, TestEngineer), RH(Member, Programmer), P(Execute), P(WriteSrc), P(ReadDocs), PA(Execute, TestEngineer), PA(WriteSrc, Programmer), PA(ReadDocs, Member), mutex(TestEngineer, Programmer)}.

假设有用户 Tom 和 Alice,其中 Tom 为 Supervisor 成员, Alice 为 TestEngineer 成员. 可以在 ABox 中添加如下断言: U(Tom), U(Alice), UA(Tom, Supervisor), UA(Alice, TestEngineer).

如果在 $TBox$ 中存在 UA 继承公理(公理 11)及静态职权分离公理(公理 16),根据初始断言 mutex(TestEngineer, Programmer), Tom 只能是以下两种情况{Member, TestEngineer, Supervisor}和{Member, Programmer, Supervisor}之一的成员.

这样 $ABox$ 有两种情况: $ABox_1 = ABox \cup$ {UA(Tom, TestEngineer), UA(Tom, Member)},或 $ABox_2 = ABox \cup$ {UA(Tom, Programmer), UA(Tom, Member)}.

本节例子说明有了 RBAC 的描述逻辑表示,可以推导出隐含的关系,并根据各种约束公理限制某些关系的产生,从而限制用户的权限,保证应用的安全.

4　结　论

本文用描述逻辑方法表示出了 RBAC 的部分性质,如与角色继承有关的 RH 传递性, UA 继承性和 PA 继承性,并且表示了约束,如静态职权分离和动态职权分离约束等. 本文给出的角色继承相关公理可以将隐含的各种关系推导出来,通过约束条件对这些关系进行限制,从而保证 RBAC 规范与访问控制策略目标一致. 解决了其他现有的 RBAC 描述逻辑方法缺乏对角色层次的合理表示及语义解释,无法表达角色继承等问题.

参考文献 (References)

[1] Finin T, Joshi A, Kagal L, et al. ROWLBAC: representing role based access control in OWL[C]//Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2008: 73－82

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

[3] Ferraiolo D, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224－274

[4] Park J S, Sandhu R S. Role-based for access control on the Web[J]. ACM Transactions on Information and System Security, 2001, 4(1): 37－71

[5] Li Q, Zhang X, Xu M, et al. Towards secure dynamic collaborations with group-based RBAC model[J]. Computer & Security, 2009, 28(5): 260－275

[6] Kwon J, Moon C. Visual modeling and formal specification of constraints of RBAC using semantic web technology[J]. Knowledge-Based Systems, 2007, 20(4): 350－356

[7] Baader F, Calvanese D, McGuinness D L, et al. The description logic handbook[M]. Cambridge: Cambridge University Press, 2002

[8] McGuinness D L, van Harmelen F. OWL Web ontology language overview[EB/OL]. MIT: W3C Recommendation, 2004 [2009-09-01]. http://www.w3.org/TR/2004/REC-owl-features-20040210/

[9] Zhao C, Heilili N, Liu S, et al. Representation and reasoning on RBAC: a description logic approach[C]//ICTAC2005, LNCS 3722. Berlin: Springer, 2005: 381－393

[10] Ji G, Tang Y, Jiang Y, et al. A description logic approach to represent and extend RBAC model[C]//1st International Symposium on Pervasive Computing and Applications. Urumqi: IEEE Press, 2006: 151－156

[11] Yu H, Xie Q, Che H. Description logic based conflict detection methods for RB-RBAC model[J]. International Journal of Computer Science and Network Security, 2006, 6(1A): 120－125

(编　辑:文丽芳)