ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.8, August 2006, pp.1804−1810
DOI: 10.1360/jos171804

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于角色访问控制管理模型的安全性分析*

杨秋伟+, 洪 帆, 杨木祥, 朱 贤

(华中科技大学 计算机学院,湖北 武汉 430074)

Security Analysis on Administrative Model of Role-Based Access Control

YANG Qiu-Wei+, HONG Fan, YANG Mu-Xiang, ZHU Xian

(College of Computer Science, Huazhong University of Science and Technology, Wuhan 430074, China)

+ Corresponding author: Phn: +86-27-87543986, Fax: +86-27-87543986, E-mail: yky_wenfeng@163.com, http://www.hust.edu.cn

Yang QW, Hong F, Yang MX, Zhu X. Security analysis on administrative model of role-based access control. *Journal of Software*, 2006,17(8):1804−1810. http://www.jos.org.cn/1000-9825/17/1804.htm

Abstract: Systemic security strategy is described by security query in administrative model of role-based access control (RBAC). According to the definition of state-transition system, security analysis is defined and executed on Turing machine. Security query is classified by necessity and possibility. As a result, necessary security query and possible security query independent of status can be resolved in polynomial time, and the conditions under which possible security query is NP-complete problem are presented, but general possible security query is un-decidable.

Key words: role-based access control; authorization management; Turing machine; NP-complete problem; un-decidable

摘 要: 在基于角色的访问控制管理模型中,采用安全查询来描述系统安全策略,引入状态变换系统定义基于角色的访问控制管理模型及其安全分析,用图灵机理论和计算复杂性理论进行安全分析.将安全查询分类为必然性安全查询和可能性安全查询,证明了必然性安全查询和与状态无关的可能性安全查询能在多项式时间内被有效解决,给出了满足 NP-完全问题的可能性安全查询的条件,而一般的可能性安全查询是不可判定的.

关键词: 基于角色的访问控制;授权管理;图灵机;NP-完全问题;不可判定性

中图法分类号: TP309 文献标识码: A

近年来,作为传统访问控制的有效代替,基于角色的访问控制(role-based access control,简称 RBAC)受到了广泛的关注.具有代表性的是 Sandhu 等人提出的 RBAC96 及其补充模型[1−3]、ARBAC97[4]、ARABC02[5]和 CL03[6]是近几年被提出来的 RBAC 管理模型.在一个大型商业系统中,角色可能成百上千,而用户则可能成千上万.对于这些角色和用户的管理不可能集中在一个小的安全组内完成,这就要求下放 RBAC 的管理权,分散授权管理,而且还要保持紧密的控制.分散式的授权管理对安全性提出了更高的要求.

在 HRU[7]中,Michael A. Harrison 等人提出保护系统主要的安全问题是权限泄露问题,并认为一般的保护系统的安全性是不可判定的.所谓权限泄露是指非信任主体取得了合法权限.RBAC 的基本思想是将权限与角色相关联,用户根据它的责任和资格被指派到相应的角色,最终获得了相应角色的权限.在 RBAC 管理模型的各种

* Supported by the National Natural Science Foundation of China under Grant No.60403027 (国家自然科学基金)
Received 2005-05-19; Accepted 2005-10-10

指派中,可能存在非信任主体执行非法的管理操作,使得非信任主体取得了合法权限.可见,权限泄露问题依然是 RBAC 管理模型中主要的安全问题.

Ninghui Li 等人在文献[8]中分析了 ARBAC97 中 URA97 组件的 AATU(assignment and trusted users)和 AAR(assignment and revocation)两类安全问题,并将安全分析归约为 RT_0 的安全分析[9],得到以下结论:半静态的 AATU 安全分析可以在多项式时间内解决,一般的 AATU 安全分析是 co-NP 难度问题;半静态的 AAR 安全分析可以在多项式时间内解决,一般的 AAR 安全分析是 co-NP 完全问题.文献[8]仅仅针对有限的两类问题进行安全分析,没有充分给出多项式时间可以解决的条件,认为一般的安全分析都是 co-NP 完全问题.

本文引入状态变换系统定义 RBAC 管理模型,将系统安全策略以安全查询方式给出,并定义了 RBAC 管理模型的安全分析.基于 ARBAC97 的 PRA97 模型,将安全查询分类为必然性安全查询(necessity security query,简称 NSQ)和可能性安全查询(possibility security query,简称 PSQ),不仅分析了权限泄露问题,而且分析了权限可用性的安全问题.对比 Michael A. Harrison 和 Ninghui Li 等人的安全性分析,证明了必然性安全查询和与状态无关的可能性安全查询能在多项式时间内被有效解决,给出了满足 NP-完全问题的可能性安全查询的条件,而一般的可能性安全查询是不可判定的.

本文第 1 节简要介绍 RBAC96 和 ARBAC97,并引入状态变换系统定义了 RBAC 管理模型.第 2 节定义了 RBAC 管理模型的安全分析,并给出了分析结论及其证明.第 3 节是全文的总结.

1 RBAC 管理模型

1.1 RBAC96和ARBAC97简介

作为本文研究工作的基本前提,本节首先简要介绍 RBAC96 和 ARBAC97.

定义 **1**. RBAC96 有以下元素:

- U:用户集;R:角色集;AR:管理角色集;P:权限集;AP:管理权限集;S:会话集;
- $UA\subseteq U\times R$,建立 U 到 R 的关联;$AUA\subseteq U\times AR$,建立 U 到 AR 的关联;
- $PA\subseteq P\times R$,建立 P 到 R 的关联;$APA\subseteq AP\times AR$,建立管理 AP 到 AR 的关联;
- $RH\subseteq R\times R$,建立 R 的偏序层次关系;$ARH\subseteq AR\times AR$,建立 AR 的偏序层次关系(通常,这种角色层次中偏序关系用"$\geq$"表示,若 $r_1\geq r_2$,称 r_1 是 r_2 的父角色);
- $user: S\rightarrow U$,是将每个会话映射到一个用户的函数;
- $role: S\rightarrow 2^{R\cup AR}$,将每个会话映射到一个角色集合,$role(s_i)\subseteq\{r|(\exists r'\geq r)[(user(s_i),r')\in UA\cup AUA]\}$.

会话 S_i 拥有权限集 $\cup_{r\in role(s_i)}\{P|(\exists r''\leq r)[(p,r'')\in PA\cup APA]\}$.

存在一个约束集合,规定了上面所列举的组件的哪些赋值被允许或拒绝.

RBAC 由许多组件组成,这些组件的管理是多面化的.ARBAC97 将管理问题划分为 3 类,通过用户-角色的指派(URA97)、权限-角色的指派(PRA97)和角色-角色的指派(RRA97)来开发不同的模型.

先决条件是 ARBAC97 中的一个关键部分,它是各种指派操作之前进行的限制检查.只有被指派的主体(用户或权限)所在的常规角色中的当前成员或非成员满足先决条件才能执行操作.以下给出 URA97 的先决条件的定义,PRA97 的先决条件有类似定义.

定义 **2**. URA97 的先决条件是一个由 x,$\neg x$,$\wedge$和$\vee$操作组成的布尔表达式,x 是一个常规角色(如 $x\in R$),先决条件由用户来核定,如果$\exists x'\geq x,(u,x')\in UA$,则 x 为真;如果$\forall x'\geq x,(u,x')\notin UA$,则$\neg x$ 为真.对于给定的角色集 R,用 CR 表示所有可能的在 R 中使用角色形成的先决条件的集合.

定义 **3**. URA97 的用户-角色指派:$can\_assign\subseteq AR\times CR\times 2^R$.

定义 **4**. URA97 的用户-角色指派回收:$can\_revoke\subseteq AR\times 2^R$.

定义 **5**. PRA97 的权限-角色指派:$can\_assignp\subseteq AR\times CR\times 2^R$.

定义 **6**. PRA97 的权限-角色指派回收:$can\_revokep\subseteq AR\times 2^R$.

定义 7. RRA97 的角色-角色指派:$can\_modify \subseteq AR \times 2^R$.

1.2 RBAC管理模型的定义

在RBAC管理模型中,无论是将用户指派到角色,还是将权限指派到角色,其本质都是用户获得相应的权限.可以将用户和角色都看成是权限的集合,在分析某个用户(或角色)是否拥有某权限时,等价于判断是否该权限被用户(或角色)拥有的权限集合所包含.为了进一步的安全性分析,我们首先定义 *Own* 函数.*Own* 函数本质是将用户和角色都看成是权限的集合.本文假定所有的指派都是显式的.

定义 **8**. 令 $S=U\cup R\cup P$.函数 $Own:S\to 2^P$,满足

1) $r\in R, Own[r]=\{p|(r,p)\in PA\}$;
2) $u\in U, Own[u]=\{p|(u,r)\in UA\wedge(r,p)\in PA\}$;
3) $p\in P, Own[p]=\{p\}$;
4) $s\in S, Own[\neg s]=P-Own[s]$;
5) $s_1,s_2\in S, Own[s_1\cup s_2]=Own[s_1]\cup Own[s_2]$;
6) $s_1,s_2\in S, Own[s_1\cap s_2]=Own[s_1]\cap Own[s_2]$.

定义 **9**(**RBAC** 管理模型). 用状态变换系统 $M=\langle K,\Sigma,\delta,Q\rangle$来模拟 RBAC 管理模型,其中:

1) K 是状态集;
2) Σ是操作集;
3) $\delta: K\times\Sigma\to K$ 状态转移函数;
4) Q 是系统策略集.

K 是状态集,例如 $k\in K,k$ 是一个六元组$\langle U,P,R,UA,PA,RH\rangle$.$\Sigma$是操作集,例如$\Sigma$是 *can_assign*,*can_revoke*,*can_assignp*,*can_revokep* 和 *can_modify* 组成的集合.状态变化函数δ定义了状态变换系统的变化规则.如果输入 t,其中 $t\in\Sigma$,系统 M 从状态 k_1 到状态 k_2,这表示当它在状态 k_1 时读入 t,转移到状态 k_2,记为 $k_1\Rightarrow_\delta^t k_2$.$k_1\Rightarrow_\delta^* k_2$ 表示状态系统 M 经过 0 次或者多次状态变化从 k_1 变化到 k_2,并且称在状态变换系统 M 中,状态 k_2 相对于状态 k_1 是可到达的.Q 是系统策略集.通常在作访问控制决策时,我们需要考虑诸如此类的安全问题:(1) 是否有不合法的用户能够取得合法权限从而导致权限泄露?(2) 是不是合法的用户取得了合法的权限从而保证操作的可执行性?我们定义的分析模型主要考虑以下两种安全策略:

1) 可能性安全策略.例如,$Own[r]\supseteq\{p\}$可能么?这一策略用于查询是否系统 M 存在某个可达状态,在这个状态下,角色 r 拥有权限 p.只有问题“非信任实体是否可能获得了合法权限从而导致权限泄露”的回答是否定的,才意味着系统是安全的.
2) 必然性安全策略.例如,$Own[r]\supseteq\{p\}$必然么?这一策略用于查询系统 M 的所有可达状态是否角色 r 拥有权限 p.只有查询“信任实体是否取得了合法的权限从而保证操作的可执行性”的回答是肯定的,才意味着系统是安全的.

2 RBAC 管理模型的安全性分析

2.1 RBAC管理模型安全性分析的定义

采用安全查询方式代替系统安全策略来分析系统的安全性是自然的.给定一个状态变化系统 $M=\langle K,\Sigma,\delta,Q\rangle$,策略集 Q 采用查询方式定义.M 在状态 k 下,如果对于查询 $q\in Q$ 被满足,记为 $k\to q$.

定义 **10**(**RBAC** 管理模型的安全分析). 对于一个给定的 RBAC 访问控制管理模型 $M=\langle K,\Sigma,\delta,Q\rangle$,如果存在$k\in K,t\in\Sigma,\phi\in\delta,q\in Q$,那么$\langle k,t,\phi,q\rangle$是一个安全分析实例.如果状态 k 的一个可达状态 k_1(即 $k\Rightarrow_\delta^* k_1$)满足 $k_1\to q$,那么称 q 是可能的,称此类查询为可能性安全查询;如果对状态 k 的任意一个可达状态 k_1(即 $k\Rightarrow_\delta^* k_1$)满足 $k_1\to q$,则称 q 是必然的,称此类查询为必然性安全查询.

每个安全策略都能形式化地转化为一个安全分析实例,在执行系统操作之前作安全分析,并且根据安全分

析的答案判定当前操作是否违反安全策略,进而接受或拒绝操作.任意的访问控制系统都有一个信任实体集 TE,这些信任实体有能力使得系统到达一个违反安全策略的状态,但它们被相信不做这样的操作.只要这些信任实体严格按照系统策略执行操作,它们执行的操作就不会违反安全策略.因此,导致系统的安全策略被破坏的情形是:$\exists u\in(u\in U-TE,(u,r_a)\in AUA)$,不属于信任实体集的管理角色用户 u 执行了 can_assign,$can\_assignp$,can_revoke,$can\_revokep$ 或者 can_modify 中的操作.

RBAC 系统中与权限直接关联的是角色,权限-角色的指派是 RBAC 管理操作中最重要的环节,也是安全分析中关键的部分.所以,本文基于 PRA97 模型展开讨论,对于 URA97 和 RRA97 也可以采用类似的分析.在 PRA97 模型中,有两类操作影响角色与权限的关联:权限-角色指派 $can\_assignp$ 和回收权限-角色指派 $can\_revokep$.

1) 如果 $can\_assignp(r_a,CR,Y)\in can\_assignp,\exists r\in Y$,那么角色 r 可拥有的权限集合将由先决条件 CR 决定;

2) 如果 $can\_revokep(r_a,Y)\in can\_revokep,\exists r\in Y$,那么角色范围 Y 中的任意角色的权限都可以被回收.

可以看出,先决条件 CR 决定权限能否被指派给角色.类似地,用户所能拥有的权限集合由先决条件 CR 和用户能够被指派到的角色所拥有的权限集合决定.因此,无论是角色还是用户,决定它们能够拥有的权限集合的关键因素是先决条件集合 CR.在本文随后的部分中,我们将对 PRA97 中的先决条件 CR 进行分析.

2.2 用图灵机对RBAC管理模型进行安全分析

在 PRA97 模型中存在着这样的一类角色,它们所拥有的权限不能从该角色中删除或增加,那么,该角色拥有的权限集合是确定的.例如,角色 r 不在任何 $can\_assignp$ 和 $can\_revokep$ 授权管理范围中出现.为了区分这类角色,我们定义成员确定的角色和成员不确定的角色.

定义 **11**. 若角色 r 拥有的权限集合不能被增加和删除,则称该角色为成员确定的角色,记为 r^D;若角色 r 拥有的权限集合可被增加或删除,则称该角色为成员不确定的角色,记为 r^U.且 $R=R^D\cup R^U,R^D\cap R^U=\varnothing$.

根据本文的定义,一个指派的先决条件是对被指派对象(用户或者权限)的成员资格的检验,分为成员资格和非成员资格的判定.而 PRA97 中的成员资格和非成员资格可以采用形式化的描述: $p\in Own[r]$或者 $p\notin Own[r]$.

通常,一个权限到角色的指派是这样的形式:$can\_assignp(x,c,Y)$,其中:$x\in AR;c\in CR$,它是由 R 的一个子集 R' 中的元素以 $x,\neg x,\wedge$和$\vee$操作形式组成的一个布尔表达式;Y 是一个指派范围.若存在 $r^U\in Y$,那么 R'中的角色能够拥有的权限集合将影响角色 r^U 能够拥有的权限集合.同时,角色 r^U 可能被包含在多个指派的指派范围内.那么,R'中的角色能够拥有的权限集合只是部分决定角色 r^U 能够拥有的权限集合.我们可以得到与角色 r^U 关联的所有集合 $R'_1,R'_2,\ldots,R'_k$.令 $R''=R'_1\cup R'_2\cup\ldots\cup R'_k$.那么,r^U 能够拥有的权限集合将被 R'' 中的角色能够拥有的权限集合和角色 r^U 当前拥有的权限集合完全决定.我们引入符号“$\perp$”指代这种决定关系:$r^U\perp r_i^D\ldots r_j^D\ r_n^U\ldots r_m^U$,表示能够指派给角色 r^U 的权限被集合$\{r_i^D,\ldots,r_j^D,r_n^U,\ldots,r_m^U\}$中的角色能够拥有的权限集合完全决定.

对任意的 $r^U\in R^U$,我们都可以得到一个与之关联的角色集合 R'',能够指派给 r^U 的权限将被集合 R'' 中的角色能够拥有的权限集合完全决定,那么可以将集合 R'' 中的成员不确定的角色用与之相关的 R''_a 中的元素集取代.为了回答两类安全性查询,如此递归下去,我们试图求解与 r^U 相关的 R^D 的某个子集合 R^{SD},而 R^{SD} 是最终决定角色 r^U 能够拥有的权限集合的成员确定的角色集合,$R^{SD}\subseteq R^D$.对于决定关系 $r^U\perp r_i^D\ldots r_j^D\ r_n^U\ldots r_m^U$,如果所有成员不确定的角色都被成员确定的角色所替代,那么关于角色 r^U 的两类安全性查询问题将得到有效解决.我们把这个替代问题转化为图灵机(TM)的语言识别问题.首先描述 TM M,它识别由 R 集合中的元素组成的字符串 w.

M=“对于输入字符串 w:

1) 从左到右扫描整个带子(tape),将形如 r^U的字符用与 r^U相关的集合 R'' 中的所有元素组成的字符串代替;

2) 如果第 1)步之后,带上只剩下形如 r^D 的字符,则接受;

3) 如果第 1)步之后,没有进行任何的置换操作,带上存在形如 r^U 的字符,则拒绝;

4) 让读写头返回带子的最左端;

5) 转到第 1)步”.

容易看出,TM M 能够识别由集合 R 中的元素组成的字符串 w,两个停机状态分别为接受状态和拒绝状态:

1) 接受状态是带上只剩下形如 r^D 的字符.这说明求解出与 r^U 相关的集合 R^{SD},而 R^{SD} 是最终决定角色 r^U 能够拥有的权限集合的成员确定的角色集合,$R^{SD}\subseteq R^D$;
2) 拒绝状态是带上还存在形如 r^U 的字符,但没有置换规则包含这些成员不确定的角色.这说明这些成员不确定的角色只包含在 *can_revokep* 的指派回收范围内,而不被任何 *can_assignp* 的指派范围所包含.

2.3 必然性安全查询的分析

事实:关于成员确定的角色的安全查询能够在多项式时间内得到有效解决.

定理 **1**. 对于 $k\rightarrow q$ 的必然性安全查询,能够在多项式时间内得到有效解决.

证明:$k\rightarrow q$ 的必然性安全查询分两种情况:(1) 如果角色 $r\in R$,并且 r 不被任意 *can_revokep* 的回收范围所包含,即角色 r 拥有的权限不能被回收,则 $k\rightarrow q$ 的必然性安全查询是具有单调性的,如果 $k\rightarrow q$,且 $k\Rightarrow^*_{op}k_n$,那么 $k_n\rightarrow q$;(2) 反之,如果角色 $r\in R$,并且 r 被某个 *can_revokep* 的回收范围所包含,即角色 r 拥有的所有权限都可能被回收,那么 $k\rightarrow q$ 的必然性安全查询的答案永远都是否定的.而判定角色 r 是否被包含在某指派回收范围内的计算复杂度则取决于 *can_revokep* 的规模,这是一个常数 C.所以,对于 $k\rightarrow q$ 的必然性安全查询,能够在多项式时间内得到有效解决. □

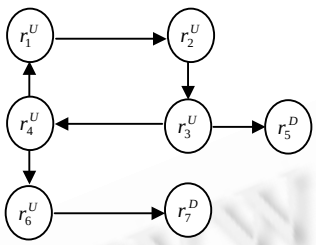

Fig.1 Decision relation "⊥" among roles

图 1 角色间的决定关系"⊥"

可以用有向图表示角色权限集合间的决定关系"⊥".例如:$T_\perp$={ $r_1^U\perp r_2^U$, $r_2^U\perp r_3^U$, $r_3^U\perp r_5^D$ r_4^U, $r_4^U\perp r_1^U$ r_6^U, $r_6^U\perp r_7^D$ }.那么,角色间的决定关系"⊥"转化为有向图 1.由图 1 我们可以看出:成员不确定的角色 r_6^U,它能够被指派的权限由成员确定的角色 r_7^D 来决定,$r_6^U\perp r_7^D$.可以知道,成员不确定的角色 r_6^U 所能拥有的权限集合被角色 r_7^D 拥有的权限集合所决定.

2.4 可能性安全查询的分析

对于可能性安全查询问题,在 TM M 上模拟 w,我们定义两类比较特殊的安全查询:使得 TM M 进入接受状态的安全查询称为与状态无关的安全查询,与状态无关的安全查询的实质是角色能够获得的权限集合能够被成员确定的角色拥有的权限集合所决定;使得 TM M 进入拒绝状态的安全查询称为回收型安全查询,回收型安全查询的实质是决定关系"⊥"右边有只被包含在 *can_revokep* 的指派范围内的成员不确定的角色出现.

定理 **2**. 与状态无关的 $k\rightarrow q$ 可能性安全查询能够在多项式时间内得到有效解决.

证明:与状态无关的安全查询,因为我们判定角色 $r(r\in R)$所能拥有的权限集合,通过 M 识别输入字符串 w,最终能够得到一个由形如 r^D 的字符组成的字符串,而这些 r^D 角色能够拥有的权限集合 $Own[r^D]$是确定的,那么,由这些权限集合通过∧,∨和¬操作得到的结果也是唯一确定的,进而可能性安全查询的结果是唯一确定的.这要求替换过程中用到所有决定关系 $r^U\perp r_i^D\ldots r_j^D\ r_n^U\ldots r_m^U$,在符号"⊥"右边的角色符号未出现在之前使用过的所有替换中符号"⊥"的左边,否则出现循环,导致不停机.假定$|w|=n$,$|can\_assignp|=m$($|A|$表示集合 A 的基数),那么,此递归操作的计算复杂度为 $O(nm)$,即能在多项式时间得到有效解决. □

定理 **3**. $k\rightarrow q$ 的可能性安全查询中的回收型安全查询问题是 NP-完全问题.

证明:从回收型安全查询的定义可以看出,回收型安全查询是使得 TM M 进入拒绝状态的安全查询问题,它的实质是决定关系"⊥"右边有只被包含在 *can_revokep* 的指派范围内的成员不确定的角色出现.若 $r^U\in R$,且 $r^U\perp r_i^D\ldots r_j^D\ r_n^U\ldots r_m^U$ 是运行 TM M 进入拒绝状态后的最终结果.

对于可能性安全查询中的回收型安全查询问题 $k\rightarrow q$,其中 q 是查询安全策略"$Own[r^U]\supseteq\{p\}$可能么?".在 $f(r_i^D,\ldots,r_j^D,r_n^U,\ldots,r_m^U)$中,形如 r^D 的字符的 $Own[r^D]\supseteq\{p\}$是确定的,所以它们被视为常量;形如 r^U 的字符,由于 r^U 被包含在 *can_revokep* 的指派范围内,$Own[r^D]\supseteq\{p\}$是不确定的,所以它们被视为变量.

令 $f(r_i^D,\ldots,r_j^D,r_n^U,\ldots,r_m^U)$表示决定关系 $r^U\perp r_i^D\ldots r_j^D\ r_n^U\ldots r_m^U$ 中角色以 x,$\neg x$,∧和∨操作形式组成的布尔表

达式,其中字母集合{ $r_i^D \dots r_j^D\ r_n^U \dots r_m^U$ }是布尔表达式中的常量或者变量.规定只有当"$Own[x]\supseteq\{p\}$"为真时,表达式中的 x 才为真.由此推演得到,只有当布尔表达式 $f(r_i^D,\dots,r_j^D,r_n^U,\dots,r_m^U)$取真值时,"$Own[r^U]\supseteq\{p\}$"才为真.这样,可能性安全查询问题"$Own[r^U]\supseteq\{p\}$可能么?"等价于布尔表达式 $f(r_i^D,\dots,r_j^D,r_n^U,\dots,r_m^U)$是否可满足的问题,即 SAT 问题,而 SAT 问题是被证明为 NP-完全问题[9].最终我们证明得到:可能性安全查询中的回收型安全查询问题是 NP-完全问题. □

同样地,我们从图 1 中可以看到,r_1^U,r_2^U,r_3^U和 r_4^U在决定关系上形成了一个环,即在图上表示为存在一个有向环路.TM M 的带子是无限长的,有向环路在 TM M 识别字符串 w 的过程中体现为循环,导致不能停机.

定理 **4**. 对于一般的 $k\rightarrow q$,可能性安全查询是不可判定的.

证明:我们将一般的可能性安全查询转化为通用图灵机语言识别的停机问题.当 TM M 停机的时候,带上只剩下形如 r^D 的字符,它们能够拥有的权限集合是确定的.那么,由它们用 x,$\neg x$,$\wedge$和$\vee$操作形式组成的表达式可以被确定,所以角色能够拥有的权限集合也被确定;当 TM M 不停机的时候,带上还保留有形如 r^U 的字符,它们是成员不确定的角色,那么角色能够拥有的权限集合也不能被确定.

若 $r^U\in R$,且 $r^U\perp r_i^D \dots r_j^D\ r_n^U \dots r_m^U$,让 TM M 识别语言 $w=r_i^D \dots r_j^D\ r_n^U \dots r_m^U$.根据前面的分析,在迭代替换过程中,M 是否停机不能判断,那么,查询某角色能够拥有的权限集合就等价于 TM M 识别语言的停机问题[10],即 HALT 问题.而 TM M 识别的语言的 HALT 问题是不可判定的,导致一般的可能性安全查询的不可判定. □

3 结束语

本文首先引入状态变换系统,形式化定义了 RBAC 管理模型,采用安全查询来描述系统安全策略,并且给出了 RBAC 管理模型安全分析的定义;定义了角色间的决定关系"$\perp$";最后用图灵机模型分析了 PRA97 中的必然性和可能性两类安全性查询,证明了必然性安全查询和与状态无关的可能性安全查询能够在多项式时间内得到有效解决.满足一定条件的可能性安全查询是 NP-完全问题,而一般的可能性安全查询是不可判定的.

RBAC 是商业中有效的访问控制技术,已经提出了许多非常完备的模型.本文对如何判定采用了基于角色的访问控制管理模型的保护系统的安全性进行了研究,这为在商业中实施 RBAC 提供了必要的理论依据,并且也为保证保护系统的安全性提供了途径.

References:

[1] Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models. IEEE Computer, 1996,29(2):38−47.

[2] Sandhu R. Rationale for the RBAC96 family of access control models. In: Youman C, Sandhu R, Coyne E, eds. Proc. of the 1st ACM Workshop on Role-Based Access Control. New York: ACM Press, 1996. 38−47.

[3] Hong F, He XB, Xu ZY. Role-Based access control. Mini-micro system, 2000,21(2):198−200 (in Chinese with English abstract).

[4] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles. ACM Trans. on Information and Systems Security (TISSEC), 1999,2(1):105−135.

[5] Oh S, Sandhu R. A model for role administration using organization structure. In: Sandhu R, Bertino E, eds. Proc. of the 6th ACM Symp. on Access Control Models and Technologies (SACMAT 2002). Monterey: ACM Press, 2002. 155−162.

[6] Crampton J, Loizou G. Administrative scope: A foundation for role-based administrative models. ACM Trans. on Information and System Security (TISSEC), 2003,6(2):201−231.

[7] Harrison MA, Ruzzo WL, Ullman JD. Protection in operation systems. Communications of the ACM, 1976,19(8):461−471.

[8] Li NH, Tripunitara MV. Security analysis in role-based access control. In: Proc. of the 9th ACM Symp. on Access Control Models and Technologies (SACMAT 2004). 2004. 126−135.

[9] Li NH, Winsborough WH, Mitchell JC. Beyond proof-of-compliance: Safety and availability analysis in trust management. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 2003. 123−139.

[10] Sipser M; Zhang LA, Wang HP, Huang X, Trans. Introduction to the Theory of Computation. Beijing: China Machine Press, 2000, 107−109 (in Chinese).

附中文参考文献:

[3] 洪帆,何绪斌,徐智勇.基于角色的访问控制.小型微型机系统,2000,21(2):198–200.

[10] Sipser M,著;张立昂,王捍贫,黄雄,译.计算理论导引.北京:机械工业出社,2000.107–109.

杨秋伟(1980－),男,湖南怀化人,博士生,主要研究领域为安全模型,信任管理模型.

杨木祥(1976－),男,博士生,主要研究领域为无线网络安全.

洪帆(1942－),女,教授,博士生导师,主要研究领域为访问控制,网络安全.

朱贤(1972－),男,博士,主要研究领域为安全模型.