基于角色的强制访问控制模型研究

田敬东[1]，何再朗[2]，王向东[3]，张毓森[4]

(1. 解放军77546部队 拉萨 850000; 2. 解放军工程兵指挥学院 江苏 徐州 221004;
3. 解放军理工大学通信工程学院 南京 210007; 4. 解放军理工大学指挥自动化学院 南京 210042)

【摘要】对传统访问控制模型进行了分析，指出它们缺点和存在的问题；介绍了基于角色的访问控制模型及其优点，提出了一种基于角色的访问控制模型，对传统的BLP模型进行改造，并给出了简要的证明。

关 键 词 访问控制; 基于角色的访问控制; 基于格的访问控制; 强制访问控制
中图分类号 TP309 文献标识码 A

Research of Access Control of Role-Based MAC

TIAN Jing-dong[1]，HE Zai-lang[2]，WANG Xiang-dong[3]，ZHANG Yu-sen[4]

(1. PLA 77546th Unit Lasa 850000; 2. PLA Engineer Command College Xuzhou JiangSu 221004;
3. Institute of Communication Engineering, PLA Univ. of Sci. & Tech. Nanjing 210007;
4. Institute of Command Automation, PLA Univ. of Sci. & Tech. Nanjing 210042)

Abstract This article analyzes the traditional access control models, points out their defects and existing problems. Particularly, a role-based access control model and its merits are introduced in this article. And then, the advanced methods of reconstructing the traditional BLP models with role-based access control model is proposed and a brief theoretical analysis is given.

Key words access control; role-based access control; lattice-based access control; mandatory access control

访问控制技术是任何安全信息系统的重要环节。访问控制主要解决系统的机密性和完整性方面的问题。20世纪70年代，Bell，Biba，LaPadula和Denning对访问控制技术领域进行基础研究，并建立了基于格的强制访问策略模型(LBAC)，其理论和概念几乎可以用到任何涉及信息流的场合。最具有代表性的两个模型是Bell-LaPadula模型(简称BLP模型)和Biba模型，被广泛应用于许多系统中。BLP模型主要解决机密性问题，Biba模型主要解决完整性问题，但是它们在实现过程中的缺陷，影响了它们的可用性。

1 Bell-LaPadula模型

Bell-LaPadula模型用强制访问控制来加强自主访问控制，以执行信息流策略。Bell-LaPadula模型的访问控制分为两步：(1) 自主访问控制矩阵***D***，但***D***的内容可以被主体修改，一个操作的实现在***D***中的验证还不够充分；(2) 操作必须被强制访问控制策略批准。

强制访问控制策略用主体和对象的安全级别来表达。用 $\lambda(s)$ 和 $\lambda(o)$ 分别表示主体s和对象o的安全级别；用 $\succ$ 表示安全级别间的支配关系，那么Bell-LaPadula模型的主要性质表现为：

(1) 简单安全特性，即当且仅当 $\lambda(s)\succ\lambda(o)$，主体$s$可以读对象$o$。

(2) *-特性，即当且仅当 $\lambda(o)\succ\lambda(s)$，主体$s$可以写对象$o$。有时也表现为严格的*-特性，即当且仅当 $\lambda(s)=\lambda(o)$，主体s可以写对象o。

但是，Bell-LaPadula模型不能完全抵抗特洛伊木马，也不能解决隐蔽信道问题[1]。

Biba模型和BLP模型没有本质的区别，都只允许安全格中一个方向的信息流，即BLP模型允许信息上流，

收稿日期：2004 - 04 - 06
基金项目：国家863计划资助项目(2002AA141090)
作者简介：田敬东(1974 –)，男，博士，主要从事信息安全方面的研究.

Biba模型允许信息下流[1]。

本文对传统的BLP模型进行改造，提出了一种基于角色的访问控制模型。

2 基于角色访问的控制模型(RBAC)

RBAC是传统的强制访问控制(Mandatory Access Control，MAC)和DAC最有希望的替换品。在基于角色的访问控制(Role-Based Access Control，RBAC)中，许可(Permission)都与角色(Role)相关。用户(User)都分配适当的角色，因而获得角色的许可，简化了许可的管理。角色可以根据一个部门的工作来创建，于是用户可以根据自身的责任和资格来分配适当的角色。用户可以方便地从一个角色被分配到另一个角色。角色可以根据应用和系统的变化授予新的许可，也可以根据需要，撤销许可。

策略中立是RBAC的一个重要特点；RBAC的另一个特点是有能力根据组织需求的变化修改策略。这些特点可以弥补BLP模型的不足。

2.1 RBAC核心模型

RBAC核心模型包括：(1) USERS、ROLES、OPERATIONS和OBJECTS分别表示用户、角色、操作和对象的集合；(2) $UA \subseteq USERS \times ROLES$ 为一个用户和角色间分配的多对多关系；(3) $(r:ROLES) \to 2^{USERS}$ 表示把角色r分配给一组用户；(4) $PERMISSIONS = 2^{(OPERATIONS \times OBJECTS)}$ 为许可的集合；(5) $PA \subseteq PERMISSIONS \times ROLES$ 为许可到角色的多对多分配关系；(6) $(r:ROLES) \to 2^{PERMISSIONS}$ 为分配的许可的集合，即把角色r映射到一组许可上；(7) SESSIONS＝the set of sessions；(8) $session\_users(s:SESSIONS) \to USERS$ 为会话用户关系，即把会话s映射到对应的用户上；(9) $session\_roles(s:SESSIONS) \to 2^{ROLES}$ 为会话角色关系，即把会话s映射到一组角色上。

2.2 角色等级模型

角色等级模型包括：(1) $RH \subseteq ROLES \times ROLES$ 是一个ROLES上的偏序关系，叫作继承关系；(2) $authorized\_users\ (r:ROLES) \to 2^{USERS}$ 即把角色r映射到当前角色等级的用户中；(3) $authorized\_permissions(r:ROLES) \to 2^{PERMISSIONS}$ 为角色r映射到角色等级上的一组许可。

3 用角色模型实现强制访问控制

3.1 基本BLP模型

LBAC中每个用户有一个唯一的安全等级，在RBAC中可以通过要求每个用户被分配两个角色r_{xR}和r_{LW}(格中最低的写等级)来实现。一个LBAC用户可以读安全等级比它低的任何对象，在RBAC中可以通过要求每个会话有两个匹配的角色r_{yR}和r_{yW}来实现。通过r_{LW}成员的特性，每个用户可以激活任何写的角色。但是，在一个特定的会话中，被激活的写角色必须和会话的写角色相匹配。因此，在RBAC中的角色等级和限制规则都被采用了。

LBAC中主要的操作是读和写。在RBAC中意味着许可是对单个对象的读和写，分别写作(o, R)和(o, W)。其他的操作与此类似。一个LBAC对象都带有一个敏感标记，在RBAC中可以通过要求每个许可对(o, R)和(o, W)分别被分配给相应的匹配角色对r_{xR}和r_{xW}。通过把许可(o, R)和(o, W)分别分配给角色r_{xR}和r_{xW}，可以明确地设定对象o的敏感标记为x。那么，可以用这些规则限制RBAC，形成如下模型：1) $R = \{r_{L_1R}, r_{L_2R}, \cdots, r_{L_nR}; r_{L_1W}, r_{L_2W}, \cdots, r_{L_nW}\}$ 表示所有角色的集合，每个安全标签由两个角色表示；2) RH由两个不相交的角色等级组成，第一个角色等级由“读”角色$\{r_{L_1R}, r_{L_2R}, \cdots, r_{L_nR}\}$组成，具有与LBAC相同的偏序关系$\succ$；第二个角色等级由“写”角色$\{r_{L_1W}, r_{L_2W}, \cdots, r_{L_nW}\}$组成，具有的偏序关系是反$\succ$；3) PERMISSIONS= $\{(o,R),(o,W)|o$是系统中的一个对象$\}$，是许可的集合；4) UA的限制规则为每个用户被分配正好两个角色r_{xR}和r_{LW}，x是被分配用户的安全标签，并且r_{LW}是根据$\succ$相应的最低安全级别的写角色；5) 会话的限制规则为每个会话正好有两个角色r_{yR}和r_{yW}；6) PA的限制规则为：(1) 如果(o, W)被分配给r_{xW}，那么(o, R)被分配给r_{xR}；(2) (o, R)只被分配给一个角色r_{xR}，x是对象o的标签。

3.2 证　明

下面证明RBAC模型满足简单安全特性和简洁*-特性。

(1) 简单安全特性

LBAC中的主体对应RBAC模型中的会话。因为主体s读对象o，则许可(o, R)必须直接或间接地分配给一个角色，而且这个角色在会话s的角色里对应一个用户u。因为u是这个会话的用户，这个角色必须直接或间接地在这个u的UA里。记 $\lambda(u)=z$ ， $\lambda(s)=y$ 。通过上面的PA限制规则，(o, R)被直接分配给唯一的角色r_{xR}，并且 $x=\lambda(o)$ 。通过RH结构，(o, R)被角色r_{yR}继承，即 $y \succ x$ 。因为s能够读o，那么在会话中必定有一个r_{yR}，通过上面RBAC模型会话角色关系定义，任何比r_{zR}低级的角色都在u的会话中，即 $z \succ y$ 。换句话说，u的会话能包括一个读角色r_{yR}，于是 $\lambda(u) \succ \lambda(s)$ 。因此，通过上面的定义证明，如果 $\lambda(u) \succ \lambda(s)$ ，并且 $\lambda(s) \succ \lambda(o)$ ，就允许主体s读对象o。这就是简单安全特性。

(2) 简洁的*-特性

每个用户u通过UA被分配给角色r_{xR}，这里x是用户的安全等级。根据LBAC，用户能读x级别或比x级别低的数据。这也意味着该用户能够开始一个x级别以下的会话。于是，如果一个用户的级别是x，想在y级别上运行一个会话，于是就有 $x \succ y$ 。上面定义的结构中的限制规则允许该会话有两个激活的角色r_{yR}和r_{yW}。因为每个用户被分配r_{LW}，那么可能每个用户都有一个会话，把r_{yW}角色作为该会话的角色之一。两个角色等级的结构表示，如果r_{yW}角色在一个用户的会话中有效，并且(o,W)在角色r_{yW}的许可里，那么用户可以写对象o。通过角色等级的结构，该会话可以向级别y或比y级别低的对象写。用LBAC的意思来表达，就是在主体s对应一个会话，在会话里，如果(o,W)在某个角色的许可里，这个写操作就可以执行，通过上面定义的结构来说就是只有条件 $\lambda(o) \succ \lambda(s)$ 满足，这个写操作可以执行。这就是简洁的*-特性。

3.3 变化的BLP模型

在变化的BLP模型里，有代表性的是具有严格*-特性的BLP模型，即当且仅当 $\lambda(s)=\lambda(o)$ ，主体s可以写对象o。那么在这个模型的RBAC改造中，也有相应的一点改变，主要表现在RH上。此时的RH由两个不相交的角色等级组成，第一个角色等级由“读”角色$\{r_{L_1R}, r_{L_2R}, \cdots, r_{L_nR}\}$组成，具有与LBAC相同的偏序关系$\succ$；第二个角色等级由“写”角色组成，没有偏序关系。其他的限制规则和上面的结构一样。

用类似证明模型满足简单安全特性和*-特性的方法，可以证明变化的BLP模型满足严格的*-特性。

本文讨论的只是BLP模型的两种。BLP模型还有多种变化，其他的变化也可以用类似的方法实现。

4 结 论

基于格的BLP模型目前还有很广泛的应用，但是它在实现过程中存在的一些缺陷，在很大程度上影响了它的可用性。本文用RBAC模型对BLP模型进行改造，既保证了BLP模型在信息流控制方面的特点，又具有RBAC模型容易管理和灵活配置的特点。

参 考 文 献

[1] Sandhu R. Lattice-based access control models[J]. IEEE Computer, 1993, 26(11): 9-19.

[2] ANSI INCITS 359-2004. Role based access control[S]. American National Standard for Information Technology, 2004.

[3] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security, 2000, 3(2): 85-106.

[4] Osborn S. Mandatory access control and role-based access control revisited[C]//In Proceedings of the Second ACM Workshop on Role-Based Access Control, New York, 1997.

编 辑 熊思亮