RBAC模型研究历程中的系列问题分析

刘 强 王 磊 何 琳
(广东工业大学CIMS重点实验室 广州 510006)

摘 要 长期以来,RBAC模型的研究工作主要集中在信息科学领域,其深厚的管理学背景与逻辑学背景并没有获得关注。在综述RBAC模型研究历程的基础上,揭示了RBAC模型存在的一系列逻辑问题与管理问题:授权状态的"伪三值逻辑"问题、管理权威的来源问题、管理员的权责同步问题、权限泄漏的含义问题、授权决策支持的模式问题。其后,从语用/语法/语义3个层面进行分析并明确了RBAC模型的二值逻辑学基础;详细阐述了系列管理问题的逻辑关系,分别分析了各个管理问题的背景和内涵,明确了管理权威的来源和权限泄漏的具体含义,提出了"有效区分分权与授权、推行权限使用审计"的权责同步思路,及"以问题求解替代安全策略与约束语义显示化"的授权决策支持模式。本研究旨在明确RBAC模型中的一些核心概念与理论基础,揭示并解决一些关键问题,为提升RBAC模型的安全性与适用性、降低RBAC模型的复杂性提供理论层面上的支持。

关键词 基于角色的访问控制,授权,安全,授权决策支持
中图法分类号 TP309.2 **文献标识码** A

Research on a Series of Problems in RBAC Model

LIU Qiang WANG Lei HE Lin
(CIMS Lab, Guangdong University of Technology, Guangzhou 510006, China)

Abstract RBAC is characterized by distributed management and self-management as the basic model in RBAC field. Today, many research themes on RBAC are almost proceeded in the field of information science, and its management and logistics background are ignored. This paper uncovered a series of management problems and logic problems existed during the research process on RBAC, including false ternary logic basis of authorized state, un-synchronization between right and responsibility of administrators, ill-defined meaning of right leakage, unclear resource of authority, and failure in decision-making during authorizing process etc. Then it analyzed the false ternary logic problem from a logic view with a three layer framework in detail, described the background, content and deriving relationships of other management problems from a management view, explained the meaning of right leakage and origin resource of authority, put forward the mechanism on the synchronization of right and responsibility and the corresponding audit system, and designed the decision support mode for the administrators when authorizing. These research can provide theoretical support for the development and update of RBAC model.

Keywords RBAC, Authority assigning, Safety, Authority assigning decision support

访问控制是信息安全领域内一个重要的研究方向,用以"确定谁对什么资源或信息能进行什么样的操作"。基于角色的访问控制模型(Role-Base Access Control,RBAC)通过定义角色这一中介语义词,建立起"用户/角色"与"角色/资源"两类映射关系,灵活地表征了用户与资源之间的访问关系。第一个形式化的访问控制模型RBAC96由Sandhu等设计[1],用以实践RBAC的这一独特的映射机制和思想。其后,RBAC96模型的管理模型——ARBAC97(Administrative RBAC)模型[2]也相继被提出,其核心思想就是在RBAC96模型中设置管理角色和管理权限,沿用RBAC96的框架实现访问控制模型的自我管理。2001年,David Ferraiolo, Ravi Sandhu等对上述RBAC模型进行了整理、提炼和标准化[3];2004年2月,美国国家信息技术标准委员会(ANSI INCITS 359-2004)将整理后的RBAC模型指定为美国的国家标准ANSI RBAC[4]。自此,RBAC96和ARBAC97模型成为了访问控制领域后续研究、改进和应用的基准模型。

长期以来,对RBAC模型的研究集中在信息科学的范畴,其逻辑学背景与管理学背景并没有得到足够的重视,对RBAC模型研究兴趣的偏向与对RBAC模型研究领域归属的默认,使其存在的一系列影响模型结构和安全性的管理问题与逻辑问题远离研究焦点,模糊不清或悬而不决。以此为目标,从逻辑学与管理学的视角揭示了RBAC模型存在的系列问题,并逐一进行了分析,提出了相应的解决思路,澄清了一些相关的基础理论,明确了一些核心概念的含义,以期为RBAC模型的进一步研究提供支持。

本文第1节着重介绍RBAC模型的研究历程及系列问

到稿日期:2012-01-24 返修日期:2012-05-08 本文受国家自然科学基金项目(61104156),广东省自然科学基金(S2011040004118)资助。
刘 强(1978-),博士,副教授,主要研究方向为访问控制技术、智能规划等,E-mail:liuqiang@gdut.edu.cn。

题产生的背景；第 2 节主要分析 RBAC 模型中的逻辑问题——授权状态的“伪三值逻辑”问题；第 3 节主要分析 RBAC 模型中存在的一系列管理问题，包括管理权威的来源问题、管理员的权责同步问题、权限泄漏的含义问题、授权决策支持的模式问题；最后总结全文，提出进一步的研究计划。

1 RBAC 模型的研究历程与系列问题

适用性、安全性、复杂性一直是访问控制模型最重要的 3 个属性。其中，适用性是指访问控制模型对应用环境的描述能力和实际控制能力，是访问控制技术得以发展的原始动力；安全性要求在访问控制过程中，禁止非法用户获得受控资源的访问权限，是访问控制最本质的要求；复杂性是对访问控制问题规模和控制难度的基本度量。这 3 大属性互依互存，左右着 RBAC 模型的研究走势。

为了巩固和提升 RBAC 模型的适用性，人们将 RBAC 模型自有体制建设和扩展作为主要研究内容：SARBAC[5] 对管理关系和管理辖域重新进行了定义和划分，解决了 ARBAC97 存在的边效应问题；负授权方式[6] 被用来提高系统对应用环境的表述能力；为了适应以分布式、协同为特征的网络应用环境，角色代理[7-9]、角色映射[10] 等相关技术被引入，并依此建立起以虚拟组织（Virtual Organization）或类似概念为暂态性的访问控制域，以多域并存、域内自治、上层策略共享为主要控制方法的协同式 RBAC 访问控制模型[11-14]。随着应用对象规模的扩大，原子访问控制事务显著增加，授权复杂性直线上升，“粒度控制”作为常规手段被广泛应用：ARBAC02[15] 针对 ARBAC97 细粒度的授权模式进行粗粒度改进，以降低其复杂性；文献[16]采用安全标签对访问控制模型的基础数据结构——访问控制矩阵中的元素进行聚合，聚合实质上是一种粒度计算，可以灵活实现访问控制的粗细粒度控制。复杂性的上升使得 RBAC 系统的安全性受到冲击，其中权限泄漏、策略违背和约束冲突等问题尤为突出。今天，RBAC 模型的安全性已经引起广泛的关注，安全策略与约束的一致性分析与检测[17-27]、安全性分析[18-35] 正逐步成为研究主流。2008 年，RBAC 模型的提出者 Sandhu 教授提炼出下一代 RBAC 模型所应遵循的 5 大原则：抽象（abstraction）、分离（Separation）、遏制（Containment）、自动化（Automation）、责任（Accountability）[36]。其中抽象与分离原则是对 RBAC96 模型特征的提炼，遏制原则（遏制恶意泄漏权限）与责任原则（提升主体的责任意识）是为了提升 RBAC 模型的安全性，自动化原则（自动授权与回收）是为了降低授权的复杂性和管理员的管理负荷，这更进一步明确了 RBAC 模型的研究方向。

在 RBAC 模型的研究历程中，相关研究主要集中在信息科学的范畴，其管理学背景与逻辑学背景并没有得到足够的重视，鲜有人深入探索与研究 RBAC 模型的管理权威来自何方——管理权威的来源问题。确定管理权威源的意义在于：可以明确 RBAC 模型中管理权限使用的汇报对象，为策略语义冲突、授权争议找到仲裁方，并为语义模糊的概念与病态定义找到最终解释人。尽管“主体的责任”已经提出[36]，但是更深入的权责概念和审计制度亟待完善，这一问题比较通俗的表述就是“RBAC 模型有效地进行了管理权限的分发与传播，却未能合理地对管理权限的使用进行监管和回收”，我们称之为安全管理员的权责同步问题。在大范围地研究安全策略与约束一致性的同时，这一研究的最终目的——“减少授权决策失误与权限泄漏、提高模型的安全性”并没有得到更完整的诠释：除了追求一致的安全策略与约束，安全管理员还期望对安全策略与约束的领域语义有更精细的把握，以期做出更加准确的授权决策。这对多域并存的协同式 RBAC 访问控制模型尤为重要。在大规模、分布式的应用背景下，要准确地把握安全策略与约束的领域语义脱离不了强有力的授权决策支持技术与工具，就需要根据安全管理员的基本授权行为，确立授权决策支持模式。然而，我们对安全管理员基本授权行为模式的认知仍处于一种简单的、缺省的共识状态——不违背约束的授权或回收操作。因此，对授权决策支持需求及延伸而来的授权决策模式就不甚清晰，这称为授权决策支持的模式问题。在执行安全分析的同时，权限泄漏的定义也不尽完善，尤其是可信主体的认定方面，缺乏清晰的判定依据，我们称之为 RBAC 模型权限泄漏的含义问题。

尽管逻辑的方法（如道义逻辑[17,18]、描述逻辑[19]、模型检测[20]）被用来进行安全策略与约束的一致性分析与检测，但是 RBAC 模型形式化的逻辑学基础仍然出现认知上的分歧和模糊，集中体现在负授权模式下授权状态的三值特性与一致性分析方法的二值逻辑基础之间的不协调，我们称之为授权状态的“伪三值逻辑“问题。

2 授权状态的“伪三值逻辑”问题

安全策略、授权状态的领域语义及其形式化总是基于某型逻辑系统而施行推理、演算等操作。常规而言，在表示授权状态时，可能存在“允许（Permit）/禁止（Refuse）/未声明（Unstatement/Null）” 3 种授权关系的赋值。如，“允许主体 O_1 访问客体 S，禁止主体 O_2 访问客体 S，对于主体 O_3 是否可以访问客体 S 不做声明”，这一现象常被直观地认为授权状态的形式化表述是以三值逻辑为基础的。不可否认的是，授权关系确实存在着 3 种赋值，其最早出现在有关负授权方面的研究文献中[6]。然而这并不意味着授权状态存在显式的 3 种语义值，“未声明”这种悬而不决的语义表述显然不符合人们对信息安全特性的基本要求——保密性（信息不能泄漏给未授权者）与可用性（授权用户随时可以访问信息）。事实上，“未声明”状态必定有其显式的含义，权限的语义赋值只存在两种形式——允许与禁止，在形式化表述与赋值后，“未声明”的权限赋值一定是其中的一种。为了说明这一现象，我们从语用/语法/语义 3 个层面上来进行解释，如图 1 所示。在表述安全状态时，根据授权赋值空间的稀疏性，人们常有选择地选用正授权模式（只记录“允许”型的授权赋值，未做记录者为“禁止”访问）与负授权模式（只记录“禁止”型的授权赋值，未做记录者为“允许”访问）。在某些应用场景，为了提高表述能力和表述的便利性，两种授权模式被混合使用。正授权和负授权两种模式下，未声明的权限都有明确的语义赋值，这显然满足封闭世界假设（Closed World Assumption，CWA）——未声明即为否定赋值。事实上，封闭世界假设就是 RBAC 模型授权状态表述的前提条件。在混合授权模式下，“未声明”状态的赋值仍然是确定的，这需要进一步确认正、负授权的主次划分。在多数情况下，混合模式总是以正授权为主，因而“未声明”状态表示禁止访问这一语义。由此可知，授权关系的三值状态只是一种语法表现；语义范畴内，RABC 的逻辑学基础屹然是二值逻辑。在实际应用过程中，混合式授权模式中负授权（以正授权为主）可以转化为 RBAC 模型中的授权约束，进而混合

式授权模式可以转化为正授权模式，这一处理过程可以使得3种授权模式获得语法上的统一。

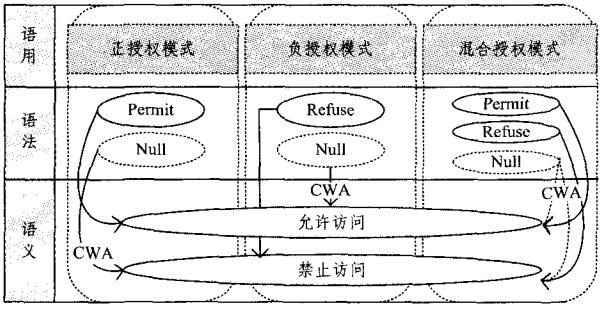

图1 RBAC授权状态的3类语法赋值及语义映射关系图

文献[37]中提到一种新的RBAC模型——BTG-RBAC。模型中，当用户申请访问控制权限得到"禁止"的回答时，用户可以冲破策略与约束的制约(Break The Glass，BTG)获得访问控制权限，其后，BTG-RBAC模型将对该主体的行为实行监控，当事主体也必须对自己的行为负责。这种从禁止访问到允许访问的转变完全得益于建立在RBAC模型的BTG机制，并不与授权状态的二值性相违背。事实上，BTG-RBAC中的授权状态仍然只存在"禁止"与"允许"两种状态。

二值逻辑基础与封闭世界假设的清晰认定，明确了RBAC模型的逻辑学基础，可以有效地引导与约束RBAC模型研究与应用过程中一些技术性方法的使用。

3 RBAC模型的系列管理问题分析

3.1 管理问题之间的逻辑关系

如前所述，RBAC模型中存在着管理权威的来源问题、安全管理员的权责同步问题、授权决策支持的模式问题、权限泄漏的含义问题等系列管理问题，这些问题之间的逻辑关系如图2所示。

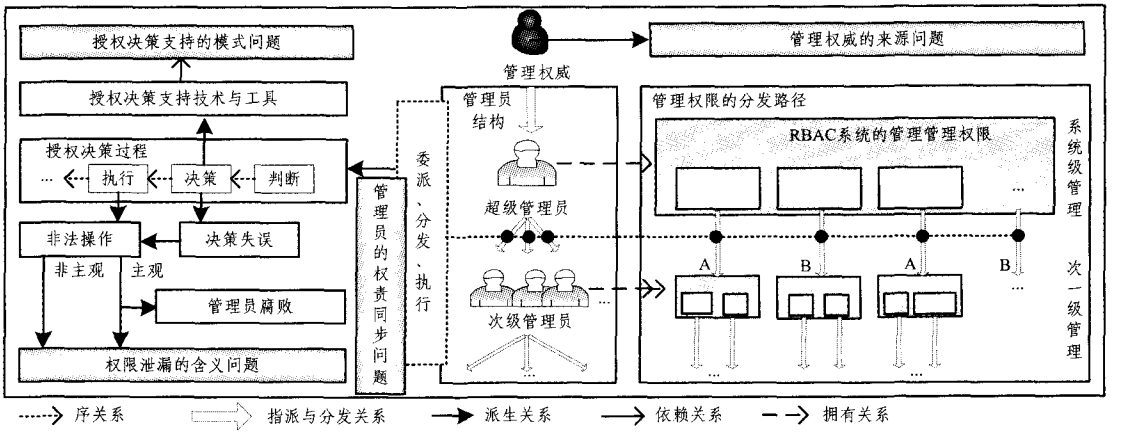

图2 RBAC模型系列管理问题的逻辑关系图

为了满足分布式管理的需求，管理权限经由管理权威向下分发与传播，这是ARBAC97模型应用实施的基础。然而，管理权威如何诞生或来自何方我们并不清楚，由此产生了管理权威的来源问题。管理权限的传播过程存在两种形式：授权过程(简称为A传播过程)和分权过程(简称为B传播过程)，两者具有不同的权责模式，RBAC模型并没有严格区分分权与授权，也没有触及责任的划分或转移，这使得各级管理员的权责不同步、不对称、不明确，一旦出现安全事故，责任的追究与划分缺乏相关政策性依据。在管理权限的委派、分发和执行过程中，各级安全管理员首先面临的就是授权决策，当管理策略的语义过于复杂和晦涩时，安全管理员就无法直观判断当前执行的管理操作的合法性，进而可能执行非法操作，导致授权决策失误和权限泄漏，这一过程涉及到权限泄漏的含义问题。为了执行正确的决策，必要的技术性的授权决策支持是必不可少的，因此，我们又不得不解决授权决策支持的模式问题。

3.2 管理权威的来源问题

如图2所示，RBAC模型存在超级管理员，所有的管理权限经由超级管理员向下委派与分发。然而，超级管理员并不是RBAC模型的管理权威。在实际的应用过程中，其尽管拥有对管理权限的委派和回收，但并非完全是管理权限使用的汇报对象，也不具备仲裁者、解释人的职能。严格而言，RBAC模型的管理权威来源于模型边界以外的权力机构，如：应用RBAC系统(以RBAC模型为访问控制模型的信息系统)的组织机构通常会指定某一用户作为RBAC系统的超级管理员，赋予其超级管理权限，尽管这一过程未必有显示的任命，但在应用系统开发或实施过程中必然做了相应的指派和认定。超级管理员因而就成为了RBAC模型的管理权威，并依据需求设置管理角色、制定安全策略、指派安全管理员等。RBAC模型的各级安全管理员将恪尽职守，向应用RBAC系统的组织机构负责，并接受其监督和考评。

由此可知，RBAC模型的管理权威正是来源于其应用对象的权力机构。只有应用对象的权力机构才能成为管理权限使用的汇报对象，而并非超级管理员。RBAC系统的各类安全策略、约束实际上经由应用对象的规章、制度、业务规则、法律法规衍生而来，在RBAC模型中得以形式化表述。因而，具有最终解释权和仲裁权的仍然是应用对象的权力机构或具有代理身份的职能部门。因此可以看出，RBAC模型中的管理事务实际是其应用对象管理事务的延续和扩展。

3.3 安全管理员的权责同步问题

管理学对分权与授权进行了严格的划分：授权是上级授予下属责任和权力，分权是组织中权力的再分配；授权是在上下级进行，分权是在同一级进行；授权者对所授权力负有责任，授权者拥有决策权，被授权者没有决策权；分权者对分配后的职责不负有责任，被分权者具有决策权，并负有全部责任[38]。多数RBAC模型的应用过程中，这种划分并没有得到重视，在淡化权责同步的意识后，分权与授权依据应用需求被混合使用。如某PDM系统采用RBAC模型进行访问控制，

系统管理员拥有最高管理权限，包括创建域、创建域管理员、进行用户到域管理员的指派等。系统管理员也需将域管理权限委派给下级域管理员，这是一个授权过程；与系统管理员并行存在的还有职能管理员，如进行论坛数据维护、信息审核等，这是一种内置式的分权方式。然而，系统并不能确认一个访问控制域发生安全事故（如技术资料泄密等）后，当事用户、域管理员、系统管理员如何承担责任，又或出现数据灾难、信息违规时，职能管理员与系统管理员各自又该承担什么样的责任。显然，事故责任的追究与划分缺乏制度支持与政策依据。

权责不同步是这一问题的具体表现。解决这一问题的关键就是要正确区分分权与授权，明确管理员的权力与责任；建立管理权限使用的审计制度，包括用于监督的常规审计与用于追究的事故审计，有效地对管理权限的使用过程实行监督与控制。这些或许并不属于RBAC模型结构性的要求，但在以安全性为最高准则的应用情景中，RBAC模型有义务在技术层面上支持包括权责同步、授权审计等在内的外围制度建设。

今天，权限泄漏导致机构、企业关键性资料泄密已足以影响到机构或企业的生存与发展。正确划分分权与授权，明确权责，建立严格的责任审计制度和事故审计制度有助于安全管理员提高责任意识，使其认真履行职责，保护信息资源的安全。

3.4 权限泄漏的含义问题

关于权限泄漏，最原始的定义来源于Harrison的论文《Protection in Operating System》[28]："an unreliable subject can not pass a right to someone who did not already have it"，意即"不可信主体不能将权限授予那些没有获得该项权限的用户"，这一定义出现在RBAC模型之前。Li等[29,30]提出信任管理领域内的安全性分析（Security Analysis）概念，其中涉及到权限泄漏概念，他们认为：不可信主体是否可以访问指定资源，如果回答为肯定，则系统存在权限泄漏。后续有关的研究在表述系统安全性或权限泄漏时，也大都涉及到主体的信任问题。其中，文献[31]通过对可能性安全策略的询问来鉴定系统安全时提到了可信主体的概念；文献[32,33]定义可达性或安全泄漏时使用了不可信用户的概念；文献[34,35]在定义可达性与可用性时所使用的指定角色（given role）或指定用户（given user）也隐式地包含可信主体的含义。信任管理（Trust Manangement，TM）的基本思想是承认开放系统中安全信息的不完整性，系统的安全决策需要依靠可信任第三方提供附加的安全信息[39]。RBAC模型最初的设计是面向封闭的组织机构，这种封闭性体现在：组织机构中各类角色或岗位受到统一的组织限制与制度约束，并以此被相互信任。这与信任管理中用户需要依靠可信第三方颁发信任凭证并与以安全策略进行一致性检测的方式迥异。RBAC模型中角色相对用户和资源的中立特性显著不同于TM模型中角色对资源的完全依附；RBAC模型中管理角色独立于常规角色的管理格局，亦不同于TM中资源拥有者自动成为资源的管理权威这一方式。因此，TM领域对于权限泄漏的定义不完全适用于RBAC模型。事实上，TM理论可以用来扩展RBAC模型的应用面（如对协同域中资源的访问控制），并提供相应的安全性验证方法，这种扩展仍然需要RBAC模型结构上的一些突破。

在RBAC模型中，各级安全管理员是可信的。管理权威或其代理在设置与指派安全管理员时，已经建立了这种信任关系，并有诸如制度和职业操守等予以维持。各级安全管理员的授权行为是合法的、必需的，但未必是安全的。鉴定其授权行为是否是安全的标准应该看这一授权行为是否遵循既定的安全策略和约束。由此，RBAC模型中权限泄漏的含义是指：RBAC管理员违背安全策略与约束，执行非法的管理操作，使得本不该拥有某项权限的用户获得该项权限。至于"谁该拥有哪项权限，不该拥有哪些权限"，则完全由组织机构的规章制度、岗位职能、业务流程等规定，并由管理权威或其委派代理者进行翻译与解释。

3.5 授权决策支持的模式问题

授权决策是访问控制模型实施与运行过程中的关键步骤。文献[40]在描述资源访问权限的请求与响应过程时，阐述了访问控制模型基本的决策方式：策略决策模块依据所提交的访问请求做出许可判断，返回决策结果，交由策略执行模块执行。这一过程仅仅体现了应用系统对已执行授权操作的效果的遵循，并没有涉及到访问控制模型自身的授权决策问题——安全管理员在执行授权操作之前所面临的授权决策问题，前者可以通过机械式的方式进行自动判断，而后者需要建立问题模型运用智能化的手段进行求解。后续有关访问控制模型决策功能方面的研究[41-43]大都局限于文献[40]所表述的决策过程。而本文关注的正是执行授权操作之前所面临的授权决策问题。

严格说来，安全策略及约束的一致性分析、安全分析具有决策支持功能。安全管理员在进行授权时，如果预先能获知所执行的授权动作的效果与既定的安全策略或约束不一致，或造成权限泄漏，即可避免不合法的操作。尽管更多的时候安全策略与约束的一致性分析仅被作为制定上层安全策略时的分析工具，但其在RBAC运行期所能提供的决策支持功能不容忽视。这在文献[21]的表述中有比较清晰的体现——授权检测（Authorization Checking）概念的提出说明了一致性分析的另一种作用方式。安全策略及约束一致性问题是比较复杂的问题。文献[22]综述了一些用于安全策略分析与验证的形式化方法或半形式化方法对RBAC各类特征的支持。文献[23]分析了约束一致性分析在分别具有互斥约束、势约束、前提约束或其组合情况下的计算复杂性，其中多数情况下是NP-hard问题。安全策略及约束一致性分析的执行也涉及多类前提假设，如对历史约束的遵循[24,25]，受控资源需要进行并发访问控制[26]等。

如第1节所述，在授权管理过程中，RBAC安全管理员仅仅知晓安全策略及约束是否一致，还不能执行正确的授权决策，还需对安全策略和约束的领域语义有比较精细的认知。如当某用户申请某项权限时，在不违背当前安全策略与约束的前提下，安全管理员仅仅依赖一致性分析结论去构造一条合法的授权路径是异常困难的，还需要更多的决策支持。文献[27]提出的用户执行路径（user' execution path）与角色需求向量（Role Requirement Vector，RRV）概念基本阐述了这一构造过程的决策支持需求。

RBAC模型的安全策略包括合法施动者、前提条件（策略的适用环境）、所允许或禁止的操作3要素。直观地去理解RBAC安全策略的语义是相当困难的：由于前提条件的存在，安全策略之间可能形成具备因果关系的可执行安全策略链（前一策略所允许或禁止的操作恰恰为后一策略的执行创造

条件),其执行效果难于直观判断,特别是大型信息系统中存在着复杂的角色继承关系,使得安全策略各个要素都可能蕴含一些隐式的子集,进而导致各级安全管理员对安全策略的辖域和执行效果的认知的非直观,在进行某些授权决策时,不能准确判断授权后的系统安全状态,从而导致决策失误,给系统带来权限泄漏或遗留安全隐患。因此,强有力的授权决策支持技术与工具必不可少,其关键就是要使得安全策略和约束的领域语义显示化。我们提出"以问题求解替代领域语义显示化"的授权决策支持模式,如图 3 所示。这一模式中,对安全管理员授权行为的分析至关重要。

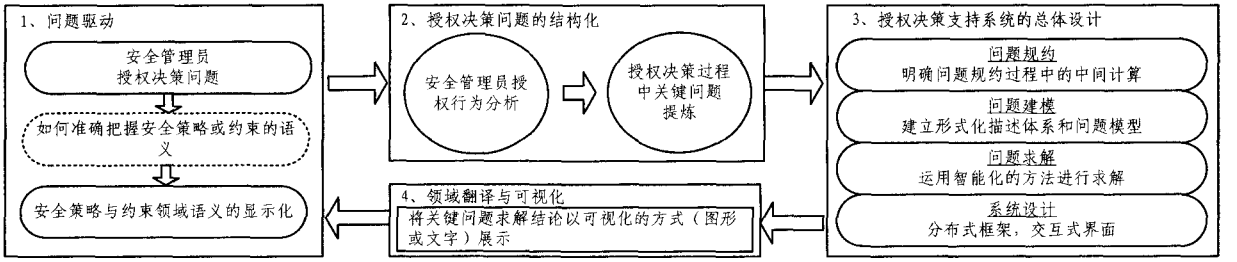

图 3 RBAC 模型授权决策支持模式

初步的研究表明,RBAC 安全管理员至少拥有 4 类基本的授权决策行为:

第一类决策行为——进行授予用户操作权限的许可判断,即判断"授予某用户某资源的访问权限"是否满足既定的约束条件,并做出许可决策。

第二类决策行为——提出合法性授权操作序列,为"授予某用户某资源的访问权限"提供满足既定约束的授权操作序列。

第三类决策行为——提出合法性管理权限委派操作序列,为"委派给某安全管理员某被控资源的管理权限"提供满足既定安全策略的委派操作序列。如果不存在委派操作序列,则不能进行委派,因而,这一决策行为涵盖了进行委派操作的许可判断。

第四类决策行为——进行安全策略和约束变更的许可判断,分析安全策略和约束的变更对已发生授权决策事件的影响,进而做出是否允许变更的决定。

第一类决策行为要求管理员判断当前授权是否满足约束,这一问题可以规约到"判断当前授权操作的效果与约束之间是否可以取得一致性的真假赋值",这是一个典型的命题可满足问题。第二、三、四类决策行为都依赖于安全管理员对安全策略和约束的语义判断和推导,其中第二、三类决策行为主要为在满足既定安全策略与约束的前提下,如何获取合法的授权操作序列,这属于经典规划问题——根据制定的目标,通过对环境的观察、分析,在满足资源限制的前提下,对若干可供选择的动作的执行顺序施行推理,得出到达既定目标的有效动作序列[44]。第四类决策行为过程中,安全管理员需要寻找与目标安全策略及约束相关的授权决策事务(第一、二、三类决策事务),然后判断相应授权操作或操作序列的合法性,进而做出变更许可,因而,第四类决策行为是第一、二、三类授权决策行为的组合或递归循环。

因此,安全策略和约束的领域语义显示化问题最终可以转化为命题可满足问题与规划问题两类科学问题的求解。

结束语 RBAC 模型及相关研究不仅隶属于信息科学的范畴,也极具深厚的管理学背景和逻辑学背景。在管理权限的委派、分发和执行过程中,存在着授权状态的逻辑学基础不明、权责不同步、授权决策失误等现象。论文从逻辑学和管理学角度深入分析了授权状态"伪三值逻辑"问题、管理权威的来源问题、安全管理员的权责同步问题、权限泄漏的含义问题、授权决策支持的模式问题,并提出了系列观点、看法与设想。论文的研究旨在明确 RBAC 模型的一些核心概念与理论基础,揭示并解决一些关键问题,为 RBAC 模型提升安全性与适用性提供理论层面上的支持。后续的研究工作将在 RBAC 模型的审计模型及授权审计制度制定方面展开,以提升各级安全管理员的责任意识;另一方面,亦将在授权决策支持系统的开发与实现等方面展开研究,部分实现授权自动化,从而降低安全管理员的授权复杂度。

参 考 文 献

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

[2] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-Based Administration of Roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135

[3] Fereaiolo D F, 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] ANSI. American National Standard for Information Technology—Role Based Access Control[C]// ANSI Int'l Committee for Information Technology Standards. Feb. 2004: 359

[5] Sandhu R, Munawer Q. A Model for Role Administration Using Organization[C]// Proceedings of the SACMAT'02. Monterey, California, USA, 2002: 155-162

[6] Al-Kahtani M, Sandhu R. Rule-based RBAC with negative authorization[C]// Proceedings of 20th Annual Computer Security Applications Conference. Arizona, 2004

[7] Zhang Xin-wen, Sejong O, Sendhu R. PBDM: A flexible delegation model in RBAC[C]// Proceedings of the 8th Symposium on Access Control Models and Technologies. Como, Itally, 2003: 149-157

[8] Stoupa K, Vakali A, Li Fang, et al. XML-Based revocation and delegation in a distributed environment[C]// Proceedings of the EDBT International Workshop on Database Technologies for Handling XML information on the Web. Heraklion, Greece, 2004: 299-308

[9] Wang He, Osborn S L. Static and Dynamic Delegation in the Role Graph model[J]. IEEE Transactions on Knowledge and data Engineering, 2011, 23(10): 1569-1582

[10] Hu Jin-wei, Li Rui-xuan, Lu Zheng-ding. On Role Mapping for RBAC-based Secure Interoperation[C]// Proceedings of 2009 Third International Conference on Network and System Security. Surfers Paradi, Austria, 2009: 270-277

[11] Lu Ya-hui, Zhang Li, Liu Yin-bo, et al. A Distributed Domain Administration of RBAC Model in Collaborative Environments [C]// Proceedings of the 10th International Conference on Computer Supported Cooperative Work in Design. Nanjing, China, 2006: 1-6

[12] Shafiq B, Joshi J B D, Bertino E, et al. Secure Interoperation in a Multidomain Environment Employing RBAC Policies[J]. IEEE Transactions on Knowledge and data Engineering, 2005, 17 (11): 1557-1577

[13] Lee H K. Towards Autonomous Administrations of Decentralized Authorization for Inter-domain Collaborations[C]// Proceedings of 2010 IEEE International Symposium on Policies for Distributed Systems and Networks. George Mason University, USA, 2010: 141-145

[14] Li Qi, Zhang Xin-wen, Xu Ming-wei, et al. Towards secure dynamic collaborations with group-based RBAC model[J]. Computers & Security, 2009, 28(5): 260-275

[15] Crampton J, Loizou G. Administrative Scope: A Foundation for Role-based Administrative Models[J]. ACM Transactions on Information and System Security, 2003, 6(2): 201-231

[16] 蔡嘉勇，卿斯汉，刘伟. 安全策略模型聚合性评估方法[J]. 软件学报，2009，20(7)：1953-1966

[17] Cholvy L, Cuppens F. Analyzing consistency of security policies [C]// Proceedings of 1997 IEEE Symposium on Security and Privacy. Oakland, USA, 1997: 103-112

[18] Frode H, Oleshchuk, Vladimir. Conformance Checking of RBAC Policy and Its Implementation[J]. Lecture Notes in Computer Science, 2005, 34(39): 144-155

[19] Huang Feng, Huang Zhi-qiu, Liu Lin-yuan. A DL-based Method for Access Control Policy Conflict Detecting[C]// Proceedings of the 1st Asia-Pacific Symposium on Internetware. Beijing, China, 2009

[20] Ninesh D, Joshi A K, Lee I, et al. Permission to speak: A logic for access control and conformance[J]. Journal of Logic and Algebraic Programming, 2011, 80(1): 50-74

[21] Crampton J, Khambhammettu H. A Framework for Enforcing Constrained RBAC Policies[C]// Proceedings of 2009 International Conference on Computational Science and Engineering. Vancouver, BC, Canada, 2009: 195-200

[22] Qamar N, Ledru Y, Idani A. Evaluating RBAC Supported Techniques and Their Validation and Verification[C]// Proceedings of 2011 Sixth International Conference on Availability, Reliability and Security. Vienna, Austria. 2011: 734-739

[23] Sun Yu-qing, Wang Qi-hua, Li Ning-hui, et al. On the Complexity of Authorization in RBAC under Qualification and Security Constraints[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(6): 883-897

[24] Hosseini A, Azgomi M A. Combination of Duty and Historical Constraints in Role-Based Access[C]// Proceedings of 2009 International Conference on Innovations in Information Technology. Al-Ain, United Arab Emirates, 2009: 309-313

[25] Wang Duo-qiang, Liu Weng-fang, Lu Jian-feng, et al. A History-based Constraint for Separation-of-Duty Policy in Role Based Access Control Model[C]// Proceedings of 2009 International Conference on E-Business and Information System Security. Wuhan, China, 2009: 1-5

[26] Xu Min, Wijesekera D, Zhang Xin-wen, et al. Towards Session-Aware RBAC Administration and Enforcement with XACML [C]// Proceedings of 2009 IEEE International Symposium on Policy for Distributed Systems and Networks. London, UK, 2009: 9-16

[27] Wang Tao, Li Wei-hua, Liu Zun. RBAC Permission Consistency Static Analysis Framework[C]// Proceedings of 2010 International Conference on Multimedia Information Networking and Security. Nanjing, China, 2010: 506-510

[28] Harrison M H, Ruzzo W L, Ullman J D. Protection in Operating System[J]. Communications of the ACM, 1976, 19(8): 461-471

[29] Li N H, Winsborough W H, Mitchell J C. Beyond proof-of-compliance: Safety and availability analysis in trust management[C]// Proceedings of of the IEEE Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 2003: 123-139

[30] Li N H, Tripunitara M V. Security analysis in role-based access control[C]// Proceedings of the 9th ACM Symposium on Access Control Models and Technologies (SACMAT 2004). 2004: 126-135

[31] 杨秋伟，洪帆，杨木祥，等. 基于角色访问控制管理模型的安全性分析[J]. 软件学报，2006，17(8)：1804-1810

[32] 刘强，姜云飞，饶东宁. 基于 Graphplan 的 ARBAC 策略安全分析方法[J]. 计算机学报，2009，32(5)：910-921

[33] 刘强，姜云飞，李黎明. RBAC 系统的权限泄露问题及分析方法研究[J]. 计算机集成制造系统，2010，16(2)：431-438

[34] Mondal S, Sural S, Atluri V. Security analysis of GTRBAC and its variants using model checking[J]. Computers & Security, 2011, 30(2): 128-147

[35] Stoller S D, Yang Ping, Gofman M I, et al. Symbolic reachability analysis for parameterized administrative role-based access control[J]. Computers & Security, 2011, 30(2): 148-164

[36] Sandhu R, Bhamidipati V. The ASCAA Principles for Next-Generation Role-Based Access Control[C]// Proceedings of 3rd International Conference on Availability, Reliability and Security (ARES). Barcelona, Spain, March 2008

[37] Ferreira A, Chadwick D, Farinha P, et al. How to securely break into RBAC: the BTG-RBAC model[C]// Proceedings of 2009 Annual Computer Security Applications Conference. Honolulu, USA, 2009: 23-31

[38] 张明玉. 管理学[M]. 北京：科学出版社，2005

[39] Blaze M, Feigenbaum J, Ioannidis J, et al. The role of trust management in distributed systems security[C]// Proceedings of Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999: 185-210

[40] Yavatkar R, Pendarakis D, Guerin R. A Framework for Policy-Based Admission Control[S]. IETF Informational Standard, RFC2753. January 2000

[41] Squair T E, Jamhour E, Nabhen R C. An RBAC-based Policy Information Base[C]// Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks. Stockholm, Sweden, 2005: 171-180

[42] Xu Min, Wijesekera D. A role-based XACML administration and delegation profile and its enforcement architecture[C]// Proceedings of the 2009 ACM Workshop on Secure Web services. New York, USA, 2009

[43] Ferraiolo D, Atluri V, Gavrila S. The Policy Machine: A novel architecture and framework for access control policy specification and enforcement[J]. Journal of Systems Architecture, 2011, 57(4): 412-424

[44] Ghalllab M, Nau D, Traverso P. automated planning theory and practice[M]. Morgan Kaufmann Publishers, 2004