基于RBAC的授权管理安全准则分析与研究

熊厚仁 陈性元 张 斌 杨 艳
(解放军信息工程大学 郑州 450001) (河南省信息安全重点实验室 郑州 450001)

摘 要 针对安全准则在授权管理安全性验证中具有的重要意义,提出了基于RBAC的授权管理安全准则。以保障授权管理的安全性为目标,分析了授权管理中的RBAC安全特性,深入剖析了授权管理安全需求,从数据一致性、授权无冗余、权限扩散可控、管理权限委托可控、满足职责分离和访问权限可用等方面给出了一致性准则、安全性准则和可用性准则3项授权管理安全准则。分析表明,该安全准则与现有的RBAC安全特性相一致,能够为基于RBAC授权管理的安全性提供有效支撑,为衡量其安全性提供标准和依据。

关键词 访问控制,授权管理,基于角色的访问控制,安全准则,职责分离,互斥
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.024

Security Principles for RBAC-based Authorization Management

XIONG Hou-ren CHEN Xing-yuan ZHANG Bin YANG Yan
(The PLA Information Engineering University, Zhengzhou 450001, China)
(Henan Key Laboratory of Information Security, Zhengzhou 450001, China)

Abstract Security principles are greatly significant to security analysis of authorization management model, but they are given little attention and are open problems. This paper proposed many security principles for RBAC-based authorization model with the aim at the security of the model. The security properties of RBAC were presented, including simple safety, simple availability, bounded safety, liveness and containment. Based on deep anatomy of security requirement in authorization management, the problems including data consistency, authorization without redundancy, controllable privilege diffusing, controllable management privilege delegating, satisfaction of separation of duty and privilege availability were discussed. The proposed security principles include consistency, security and availability principles. Analysis result indicates that the security principles are consistent with the security properties of RBAC, which can support the security requirements of authorization management efficiently and provide criterions for evaluating the security of RBAC-based authorization model.

Keywords Access control, Authorization management, Role-base access control, Security principles, Separation of duty, Mutually exclusive

1 引言

基于角色的访问控制(Role-Based Access Control, RBAC)[1-3]是继自主访问控制(Discretionary Access Control, DAC)和强制访问控制(Mandatory Access Control, MAC)发展起来的一种访问控制模型。通过引入角色这一概念,RBAC模型实现了用户与权限的逻辑分离,用户不直接与权限相关联,而是通过角色获得所需权限。由于具有灵活、便于管理和策略中立等优点,RBAC已成为目前应用最为普遍的访问控制模型之一,并成为学者们研究的热点[4-14]。

在访问控制领域,安全分析的目的是确保访问控制策略的执行不会将权限泄漏给未授权用户,是保证访问控制策略能够有效执行的基础。目前,对RBAC模型安全性分析的研究较多[4-13],如Munawer和Sandhu[4]、Crampton[5]分别于1999年和2002年研究指出RBAC96中的简单安全问题是不可判定的。Koch等人[6]采用图变换方法对DAC和RBAC的安全性进行分析,并指出在访问控制规则上增加合理的约束可使其安全分析问题是可判定的。Li Ninghui等人[7,8]对RBAC模型的安全性分析问题(Security Analysis)进行了精确定义,针对AATU(Assignment and Trusted Users)和AAR(Assignment and Revocation)两类问题对ARBAC97模型进行了安全分析。Sasturkar等[9]运用智能规划技术对ARBAC的安全策略进行安全性分析,运用图规划算法求解规划问题,得出可达性问题属于PSPACE-Complete问题的结

到稿日期:2014-04-16 返修日期:2014-07-09 本文受国家"863"高技术研究发展计划(2012AA012704),国家"973"重点基础研究发展计划(2011CB311801),河南省基础研究计划项目(142300413201),河南省科技创新人才计划(114200510001)资助。
熊厚仁(1986—),男,博士生,主要研究方向为授权、访问控制与资源管理,E-mail:xionghouren@163.com;陈性元(1963—),男,博士,教授,主要研究方向为网络信息安全;张 斌(1969—),男,博士,教授,主要研究方向为网络信息安全;杨 艳(1973—),女,硕士,副教授,主要研究方向为网络信息安全。

论。Muhammad等[10]分析了ABAC模型中的互斥角色和互斥权限问题及其对安全性的影响。Anna等[11]利用程序验证工具(program verification)从RBAC的管理模型ARBAC(Administrative Role-Based Access Control)中的角色可达性入手对其安全性进行了分析。Ping Yang等[12]分析了ARBAC中无独立管理员的情况下用户-角色可达性问题,并指出用户-角色可用性、角色包含等问题均可转化成该问题加以分析。Xiaofan Liu等[13]从负授权角度分析了核心RBAC及层次RBAC模型中的授权问题并采用DATALOG语言进行了描述。

综上分析可知,常用的RBAC的安全性分析方法有自动机理论、Petri网、图变换技术、智能规划技术等[4-14]。虽然研究方法各异,得出的结论也略有不同,但大多表明其简单安全分析问题是难解的或不可判定的,且研究结论主要集中于实施安全分析的计算复杂度及可判定性方面。然而,几乎所有的研究都没有直接针对判定某访问控制系统是否安全这一问题展开。现有附加安全约束和限制来保证RBAC安全性的研究也主要集中于约束和限制的表达,对于如何执行授权管理操作才能确保这些约束或限制得到满足的研究则较少,且模型应遵循的安全约束也没有统一的标准,模型所遵循的限制和约束对应于已有的哪些授权安全属性也没有给出相应的说明。

针对以上问题,文献[14]从可能给授权管理带来的安全风险、不一致现象角度分析了授权管理的安全需求及其对授权管理安全性的影响,进而提出了与现有RBAC安全性要求一致的授权管理安全准则,并基于该安全准则分析了所提出授权管理模型的安全性。该文献不仅指出模型的安全性是可判定的,同时得出了模型安全的结论。然而,该文仅考虑了与基于RBAC的角色授权管理部分的安全需求相应的安全准则,没有考虑用户授权管理部分应满足的安全需求;且将授权管理安全准则分为一致性准则、权限无泄漏准则和职责分离准则,分类方法有待完善;未考虑模型操作可能造成的孤立角色而破坏授权数据的一致性。

本文在文献[14]的研究基础上进一步分析了基于RBAC的授权管理的安全需求,提出与这些安全需求相对应的基于RBAC的授权管理安全准则,包括安全性准则、一致性准则和可用性准则3个方面,对该文献提出的授权管理安全准则进行扩展和完善。这些安全准则可为基于RBAC模型的授权管理的安全性提供有效支撑,为衡量授权管理模型的安全性提供标准和依据,为模型安全性的形式化验证奠定基础。

2 授权管理的安全性分析

授权管理模型的安全性是保证模型安全、有效运行的关键,是访问控制目标实现的前提。而授权管理安全准则则是授权管理模型安全性验证的基础和依据。

安全分析(Safety Analysis)理论主要用来分析和测定访问控制系统是否存在权限泄漏。最初的安全分析定义为:安全的访问控制系统经执行命令序列后,是否可到达不安全的状态,使得原来不曾拥有访问权限的主体可以访问受控资源,从而导致权限泄漏。1976年,Harrison证明在HRU模型[15]中安全分析问题是图灵停机问题(Halting Problem),是不可判定的。但在一些特殊的条件下,如不允许增加主客体、单原子操作的命令集等情况下可转化成可判定问题。因此,分析访问控制系统是否存在权限泄漏是评定访问控制系统安全的关键。其中,权限泄漏是指非法主体获得受控资源的操作许可[16]。此后,访问控制领域的许多安全问题都采用这一定义和思想对访问控制模型的安全性进行分析验证。

在BLP模型中,安全性提出之初就给出了明确定义[17],包括:简单安全性、*-特性、自主安全性、兼容性,系统对所有的主体和客体都分配一个包含密级和范畴集的安全级,并通过主客体的安全级控制主体对客体的访问。Biba模型也有与BLP类似的明确定义的一系列安全属性或安全准则。

与BLP、Biba不同,RBAC模型在提出时并没有明确定义其安全特性,而后续研究者在对RBAC进行研究的过程中给出了相关理解和定义。其中,比较经典的是斯坦福大学Li Ninghui教授等于2004年提出的RBAC模型中安全性分析(Security Analysis)的概念[7,8],包括以下5个方面。

(1)简单安全问题(Simple Safety):即最早的安全分析问题,又称为可达性(Reachability)问题,主要分析是否存在某一状态,该状态下不可信用户包含在对指定资源具有访问权限的用户集中,其否定回答表示系统是安全的。该定义用于判断是否存在某一状态,未授权的不可信用户能够访问资源,即是否存在权限泄漏。

(2)简单可用性(Simple Availability)问题:分析在所有可达的系统状态中,用户是否总是可以访问指定资源,其肯定回答表示系统是安全的。该定义用于判断系统的任意可达状态中,用户是否总能够访问目标资源,即任意授权用户总是可以使用被授予的访问权限访问指定资源,强调资源访问权限的可用性。

(3)限定安全性(Bounded Safety)问题:分析在所有可达的系统状态中,可以访问指定资源的用户集U_1受到另一个用户集U_2的限制,其肯定回答表示系统是安全的。RBAC模型中的互斥性就是限定安全性问题的一个特例,即在所有可达的系统状态中,可以访问某一资源的用户集U_1和可以访问另一资源的用户集U_2之间不存在交集,其肯定回答表示系统是满足互斥性的。该定义用于判断系统是否满足职责分离,支持职责分离安全原则是RBAC的一个重要特性,系统满足了职责分离原则时,即满足限定安全性。

(4)活性(Liveness)问题:分析在所有可达的系统状态中,可以访问某一资源的用户集U总是存在至少一个用户,其肯定回答表示与用户集U相关的资源是保持活性的。该定义用于判断系统的所有可达状态中,是否资源总是至少能够被一个用户访问,这实际强调的是资源访问权限可被分配给用户的性质,同时也强调了资源的可用性。

(5)包容(Containment)问题:分析在所有可达的系统状态中,如果用户已经具有某一属性也必然具有另一属性,其肯定回答表示系统是安全的。比如,在RBAC状态中,某一权限p是角色r的有效权限,判断在每一可达状态中,是否任意具有权限p的用户都拥有角色r,其肯定回答表示系统是满足包容性的。

该概念自提出后被大多数研究者所认可并沿用。其中的简单安全性与Harrison给出的安全性定义相对等。

Li Ninghui教授对RBAC安全性定义中的安全属性与基于RBAC的授权管理过程密切相关。因此,基于Li Ninghui

教授给出的 RBAC 安全性定义对基于 RBAC 的授权管理安全准则进行了分析。

3 基于 RBAC 的授权管理安全需求

基于 Li Ninghui 教授对 RBAC 安全性的定义，从授权数据的一致性、权限分配和委托的安全性及资源访问权限的可用性 3 个方面对基于 RBAC 的授权管理安全需求进行分析，分析授权管理过程中可能带来的安全风险、不一致现象以及不满足这些安全需求可能造成的不安全后果。

3.1 授权数据及其关系的一致性

授权数据及其关系的一致性需求是强调整个授权管理过程中所有的管理操作必须保证授权数据的一致性，授权管理对象及其映射关系应该保持一致，不应存在冗余的对象和授权信息。

(1)授权数据一致

授权管理过程中，授权管理操作应与授权管理对象及其映射关系保持一致，即用户、角色、会话、资源、资源操作、资源访问权限、用户角色分配和角色权限分配中各项数据的对应关系应保持一致。与角色对应的权限应是有效权限，由有效的资源和有效的资源操作构成，而分配给用户的角色应是具有有效权限的角色；同样，由有效资源和操作构成的权限也一定是可以被指派给角色的有效权限，具有有效权限的角色也可以供用户使用。当将资源或资源操作删除时，与此对应的访问权限也应随之删除，由显式授权或隐式授权获得这些权限的角色也应将这些权限撤销，以保证角色所对应的权限是有效的；当将角色删除时，获得此角色的用户应将对角色的权限撤销，使得用户持有有效的角色和访问权限。

如图 1 所示，假设权限 p_1 由资源 res_1 和资源操作 op_1 构成，并被授予角色 r_3，并且自动被上级角色 r_1 和 r_2 继承获得。当系统安全策略发生变化，需要将资源 res_1 或对其的操作 op_1 从该授权管理系统中删除时，应同时将由此资源和操作构成的权限 p_1 一并删除，并从 r_1、r_2 和 r_3 处撤销该权限，否则将导致任何持有角色 r_1、r_2 或 r_3 的用户均具有对资源 res_1 的操作权限，与新的应用需求和系统安全策略不相适应，且容易造成信息泄漏。因此，授权管理操作应保证操作执行前后授权数据的一致性，操作执行能够很好地与授权管理需求相适应。

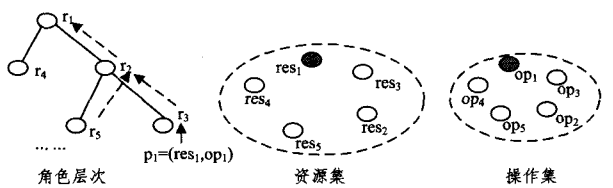

图 1 授权数据一致性

(2)权限和关系无冗余

权限和关系无冗余是指在授权管理过程中，应保证删除角色或权限后，系统中不会存在威胁系统安全的用户授权信息 UA、角色授权信息 PA 或角色互斥关系等冗余授权数据。

由于继承关系的存在，基于 RBAC 的授权管理中存在显式授权和隐式授权，在为角色分配对指定资源的访问权限时，容易导致角色对应的权限集存在重叠现象；同样，当为用户分配多个角色时，具有继承关系的两个角色之间的重复权限也将出现在用户的权限集中。这些冗余授权数据的存在，不仅降低了管理效率，也存在安全隐患，容易造成权限撤销时操作失效或遗漏，最终导致权限泄漏。

如图 2 所示，由于权限 p_1 隐含权限 p_2、p_3 和 p_5，如果为角色 r_3 分配权限 p_1，则隐含将权限 p_2、p_3 和 p_5 授予角色 r_3，同时上级角色 r_1 和 r_2 也隐式地获得这些权限；若再显式为角色 r_3 分配权限 p_2，则隐含将权限 p_3 和 p_5 授予角色 r_3，上级角色 r_1 和 r_2 同样继承这些权限。这样，角色 r_1、r_2 和 r_3 的权限集中的权限 p_2、p_3 和 p_5 出现重叠现象。此时，当显式地撤销角色 r_3 的权限 p_1 时，由于重复授权的存在，角色 r_1、r_2 和 r_3 仍持有权限 p_2、p_3 和 p_5，导致权限撤销失效，而这些权限的冗余容易带来权限泄漏等安全隐患。

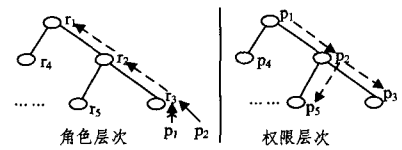

图 2 授权数据撤销时权限冗余

在角色层次中，当删除下级角色或角色间的继承关系时，由于继承关系得到的互斥关系也应及时删除。如图 3 所示，角色 r_5 和 r_6 之间存在互斥关系，由于继承关系的存在，角色 r_1 继承 r_5 的所有权限及其关系，使得 r_1 和 r_6 之间也存在互斥关系。当角色 r_5 从系统中删除或角色 r_5 与 r_2 的层次关系被删除时，冗余的互斥关系(r_5，r_6)和(r_1，r_6)也应得到及时删除。

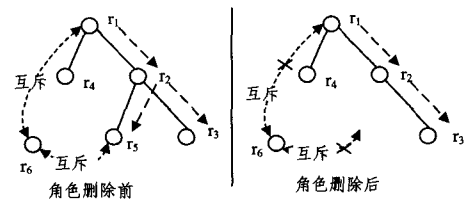

图 3 角色删除时互斥关系冗余

(3)无孤立角色和权限存在

由于角色和权限层次关系的存在，当删除角色或权限时，易造成孤立角色或权限的存在，此时应将孤立的角色节点或权限节点一并删除，或为其指定新的父节点，以避免造成冗余的对象信息。

如图 4 所示，角色 r_1 与 r_2、r_2 与 r_3 和 r_2 与 r_5 之间存在角色继承关系，当删除角色 r_2 时，角色 r_3 和 r_5 成为了孤立节点，如果不将其同时删除或指定新的父角色，将使其成为无效角色。

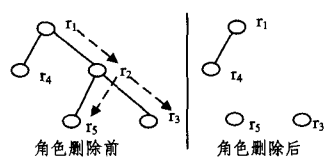

图 4 角色删除后导致孤立角色存在

3.2 权限分配和委托的安全性

授权管理的安全性是指在用户-角色的分配、角色-资源访问权限的分配和权限委托过程中，应保持权限的可管可控，不会造成权限泄漏及不安全现象的发生。

(1)权限扩散的可控制

权限扩散的可控制指在授权管理过程中，由于角色层次关系、资源层次结构等可能带来隐式授权，该隐式授权带来的权限扩散不会违背模型的安全约束，不会造成权限的非预期授予从而导致权限泄漏，且隐式授权所获得的访问权限也是可撤销的。

首先，考虑隐式授权可能带来的违背模型安全约束和权限的非预期扩散情况。为简化授权管理，基于 RBAC 的授权管理模型都支持角色层次关系从而使得权限可沿角色层次被上级角色自动继承；同时，资源本身可能存在的层次结构也容易带来权限的隐式授予。当显式授予角色某一权限时，可能隐式地授予该角色多个权限；而当为某一用户显式分配角色时，可能会使该用户获得该角色及其子角色对应的所有权限，从而造成权限扩散，容易带来安全威胁。因此，权限授予和分配时，应能够控制权限扩散的范围，避免产生违反模型的安全约束和非预期的权限授予情况。

如图 5 所示，假设角色 r_5 和 r_6 互斥。在不考虑隐式授权的情况下，将角色 r_1 和 r_6 同时授予用户 u 是可行的，不会引发安全问题；但当考虑隐式授权时，由于角色 r_5 和 r_6 互斥，角色 r_1 通过 r_2 继承 r_5 的权限，使得角色 r_1 和 r_6 也存在互斥关系，当同时将 r_1 和 r_6 分配给 u 时，违背了静态职责分离约束，存在极大的安全隐患。这种情况应加以避免。

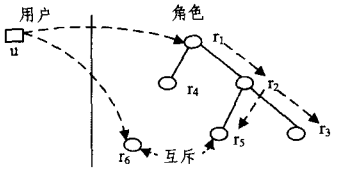

图 5　权限扩散导致违反职责分离安全约束

如图 6 所示，假设为角色 r_3 授予权限 p_1，由于角色层次中的继承关系，p_1 会沿着角色层次关系依次被上级角色 r_1 和 r_2 继承；而在权限层次中，由于权限 p_1 隐含权限 p_2、p_3、p_5，这些权限也随着 p_1 被授予 r_3，同时也随 p_1 被 r_3 的上级角色继承而被 r_1 和 r_2 继承，造成了权限的大范围非预期扩散，存在较大的安全隐患。安全的授权管理应能准确控制这种权限扩散的范围，避免造成权限的非预期授予和扩散。

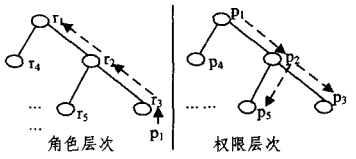

图 6　权限扩散导致的非预期授予

其次，考虑隐式授权的权限撤销问题。在权限撤销过程中，显式授权的权限被撤销的同时，通过隐式授权获得的该权限也必须相应地自动撤销，从而避免权限的不可控制。在如图 6 所示的角色层次中，当 p_1 被授予角色 r_3 时，r_3 的上级角色 r_1 和 r_2 也通过继承隐式获得权限 p_1。当撤销角色 r_3 的权限 p_1 时，为保持权限的可管可控，权限 p_1 也应从 r_1 和 r_2 处撤销。继承的权限应跟随继承源权限的撤销而撤销。

(2)权限委托可管可控

为减轻授权管理负担，授权管理支持授权委托，即允许管理员将部分管理权限委托给其他管理员，并在规定的时间范围内将委托的管理权限及时回收。在管理权限委托和回收过程中，应保证管理权限不会发生非预期的更改或泄漏，即管理权限的委托不会超出预期想要委托的权限，同时回收的权限不会少于预期准备回收的权限。

进行权限委托时，管理员不能将其没有的权限委托给其他管理员，撤销委托时则应保证所委托的权限全部回收。只有担任系统管理员角色的管理用户才具有将其管理权限委托给具有其下级系统管理角色的管理员，且只有其所支配的管理范围的下级管理权限委托出现；当删除下级系统管理角色时，应将子管理范围的管理权限全部回收。

(3)满足职责分离约束

RBAC 模型通过互斥角色约束实现职责分离原则，但无法验证是否实现了职责分离。职责分离原则强调至少有 n 个用户才能拥有一组具有利益冲突关系的权限集中的所有权限，而单个或少于 n 个用户则只能拥有其中的部分权限；互斥角色约束将组内具有冲突关系的权限授予不同的角色从而构成互斥角色集，通过限制用户只能拥有该角色集中的一部分角色达到支持职责分离的目的，但用户拥有了这些互斥角色集中的哪些权限没有得到约束，导致用户的权限得不到控制。授权管理中的角色授权主要负责为角色授予对指定资源的访问权限，应对职责分离中权限的分配情况、互斥角色约束中角色能够拥有的权限进行合理的限制，从而保证整个授权管理过程能够支持并满足职责分离；而负责为用户指派角色的用户授权则应能保证用户不会同时获得互斥角色集中的两个或两个以上角色。

如图 7 所示，假设职责分离策略为$\langle\{p_1,p_2,p_3\},2\rangle$，表示权限集中的权限至多只能有两个权限可同时被同一用户拥有；互斥角色约束为(r_3,r_5)，表示角色 r_3 和 r_5 不能同时授予同一个用户。此时，为角色 r_5 分配权限 p_3，为角色 r_3 分配权限 p_1 和 p_2，并限制这些权限不能被上级角色继承，通过互斥角色约束(r_3,r_5)可限制用户不能同时拥有$\{p_1,p_2,p_3\}$中的所有权限，从而实现职责分离。

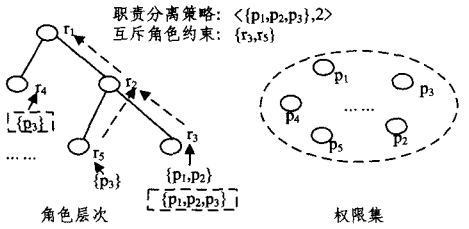

图 7　职责分离原则示例

然而，有些情况仅仅通过互斥角色是无法完成的。如图 7 中，若允许分配给角色 r_3 和 r_5 的权限可被上级角色继承，则角色 r_2 可通过继承获得权限集$\{p_1,p_2,p_3\}$中的所有权限，从而违背职责分离策略；同时，若直接将权限集$\{p_1,p_2,p_3\}$分配给角色 r_3，则不管采用互斥角色约束(r_3,r_5)还是其他措施限制用户-角色的分配，都将无法限制用户对权限集$\{p_1,p_2,p_3\}$中所有权限的持有，任何拥有角色 r_3 的用户都将获得该权限集中的所有权限，从而违背职责分离策略；另外，当为角色 r_3 分配权限 p_1 和 p_2，为角色 r_5 分配权限 p_3 时，通过互斥角色约束(r_3,r_5)限制用户-角色的分配将无法达到满足职责分离的目的，任何同时拥有角色 r_3 和 r_4 的用户都将获得权限集$\{p_1,p_2,p_3\}$中的所有权限，违背职责分离策略。

可见，授权管理中的角色授权过程为角色分配哪些权限是系统是否满足职责分离原则的关键。角色授权应为角色分

配合理的权限，使系统在满足互斥角色约束时就能保证系统满足职责分离原则。同样，用户授权过程不仅需要避免为同一用户授予互斥角色，也应避免为用户分配的角色不会继承两个互斥角色，从而有效确保冲突权限的分离。

3.3 资源访问权限的可用性

可用性是指在整个授权管理过程中不会出现无效的角色、权限和资源，即只要由有效资源和资源操作构成的权限都是有效的，可被授予角色，而通过用户授权获得持有该权限的任何用户都能使用该权限对指定资源进行访问。

(1)不会存在无法访问的权限

给定一个有效资源，用户总能通过角色获得对该资源的访问权限，强调资源访问权限的可用性；对于任一有效权限，总存在一条授权路径可使用户获得该权限，强调资源访问权限可被有效分配。

用户、角色、资源、资源操作和权限等任一授权管理对象均应属于某一授权管理范围并被授权管理员管理，不会存在无法管理的对象和关系。当删除某管理角色时，应将其管理范围及其管理权限及时回收，不会造成管理范围失控或无法管理的情况。

(2)权限不会被非预期撤销

任何通过合法授权获得访问权限的用户都能有效地使用所获得的权限访问指定资源，不会存在非预期的拒绝访问情况。由于角色继承关系的存在，上级角色可从下级角色继承获得访问权限，当将显式授予某角色的权限撤销时，由于该权限已被上级角色继承，这些继承权限也会随之被撤销，这样可能导致上级角色从其它子角色处继承得到的这些权限也相应被撤销，造成可用权限被意外撤销，导致原本有效的权限意外失效。

如图 8 所示，权限 p_1 隐含权限 p_2、p_3 和 p_5，若为角色 r_3 分配权限 p_2，则隐含将权限 p_3 和 p_5 授予角色 r_3，同时上级角色 r_1 和 r_2 也隐式地获得这些权限；若再显式为角色 r_2 分配权限 p_1，则隐含将权限 p_2、p_3 和 p_5 授予角色 r_2，上级角色 r_1 继承这些权限。此时，若显式撤销角色 r_3 的权限 p_2，则 r_1 和 r_2 所持有的权限 p_2、p_3 和 p_5 也将被随之撤销，导致 r_1 和 r_2 从权限 p_1 获得的这些合法权限无法正常使用，破坏了资源访问权限的可用性。

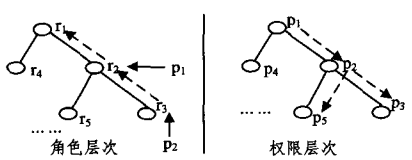

图 8 权限非预期撤销

4 基于 RBAC 的授权管理安全准则

基于 Li Ninghui 教授对 RBAC 安全性的定义，结合授权管理安全需求，从授权的安全性、一致性和可用性 3 方面给出基于 RBAC 的授权管理安全准则。

4.1 一致性准则

一致性是确保授权过程安全的最基本要求，只有保证了授权管理操作的正确性和一致性，才能进而确保模型的安全。在授权执行过程中，管理操作应保持授权数据的一致性要求，避免授权冗余要求和无孤立角色与权限存在要求，进而确保管理操作的正确性和一致性。

定义 1(授权数据一致性) 当满足以下条件时，称授权管理满足授权数据一致性要求。

(1)若权限 $p=(res,op)$ 是可被授予或已被授予角色的有效权限，则 res、op 分别是系统内的有效资源和资源访问操作；反之若 res、op 分别是系统内的有效资源及其访问操作，则对应的权限 $p=(res,op)$ 一定是可被授予角色的有效权限。

(2)若 r 是已被授予有效权限 p 的角色，则 r 是可被分配给用户的有效角色；反之，若 r 是已被授予用户的角色，则 r 一定是有效角色，其对应的权限 $p=(res,op)$、资源 res 和资源访问操作 op 也一定是有效的。

该条件要求被授予角色的权限一定是有效权限，且对于将要指派的权限也一定是符合系统当前状态的有效权限，确保只有有效权限才能被授予角色，进而授予用户。非授权管理范围内的资源不能作为授权对象。授权管理需要与应用需求始终保持一致，并随着应用需求和安全策略的变化而变化。授权管理能够始终保持授权数据的一致性，从而保证授权管理操作执行的正确性和安全性。

定义 2(授权无冗余) 当满足以下条件时，称授权管理满足授权无冗余要求。

(1)角色授权条件：假设权限 p_1 蕴含的权限集为 $P_1=\{p|p_1\succ p\}$，$p_1\succ p$ 指权限 p_1 蕴含 p，权限 p_2 蕴含的权限集为 $P_2=\{p|p_2\succ p\}$，若为角色 r 显式授予权限 p_1，为角色 r 的任一下级角色 r_1 显式授予权限 p_2，则应满足 $P_1\cap P_2=\varnothing$；

(2)用户授权条件：假设角色 r_1 持有的权限集为 P_1，角色 r_2 持有的权限集为 P_2，r_1 和 r_2 不是互斥角色，若为用户 u 同时授予角色 r_1 的任一上级角色 r_3 和 r_2 的任一上级角色 r_4，则同样应满足 $P_1\cap P_2=\varnothing$。

该条件要求授予角色和用户的权限不存在重叠和交叉现象，保证有效权限集是最简的，以更利于权限撤销等管理操作，有效避免权限泄漏问题的发生。

定义 3(关系无冗余) 当满足以下条件时，称授权管理满足关系无冗余要求。

假设集合 O 为授权管理对象集，其中授权管理对象包括角色、资源、资源操作、权限等，O 上存在二元关系 DR，则 R 应满足：若 $(o_1,o_2)\in DR$，则 $(\exists o_3)((o_1,o_3)\in DR\wedge(o_3,o_2)\in DR)$ 不成立。

该条件要求角色、资源、资源操作、权限等授权管理对象之间的二元关系不存在冗余，使得关系尽可能简单，并保证关系管理不会导致管理操作失效。授权管理操作应确保任何被授予用户的访问权限都是可被使用的有效权限，不会发生访问权限无法正常使用的意外情况。

定义 4(不存在孤立角色和权限) 当满足以下条件时，称授权管理满足不存在孤立角色和权限要求。

假设集合 O 为角色、权限等授权管理对象集，偏序关系 $o_0\succ o_1\succ\cdots\succ o_i\succ o_j\succ o_k\succ\cdots\succ o_n$ 为对象间层次结构的一部分，当将层次结构中的对象元素 o_j 删除时，为 o_k 定义新的父节点 o_i，得到新的偏序关系 $o_0\succ o_1\succ\cdots\succ o_i\succ o_k\succ\cdots\succ o_n$，避免 $o_k\succ\cdots\succ o_n$ 节点成为孤立节点而得不到有效管理。

该条件要求授权管理过程中，角色或权限的删除操作不会导致不可管理的角色节点或权限结点出现，导致角色或权限的不一致和授权管理操作失效。

4.2 安全性准则

安全性是授权管理正确、有效执行的关键。授权管理应确保授权-角色分配、角色-权限分配和权限委托过程中的安全性，保证不会发生权限泄漏。基于 RBAC 的授权管理应满足权限扩散可控要求、权限委托可管可控要求和满足职责分离要求。

定义 5(权限扩散可控) 满足以下条件时，称授权管理满足权限扩散可控。

(1)若 r_1 为支配 r_2 的任一角色，即 $r_1 \succ r_2$，p_2 为被 p_1 蕴含的任一权限，即 $p_1 \succ p_2$，当为角色 r_1 授予权限 p_1 时，该授权产生的扩散权限为 $\{(r,p) \mid (r,p) \subseteq R \times P\}$，其中 $R=\{r_1 \mid r_1 \succ r_2\}$，$P=\{p_2 \mid p_1 \succ p_2\}$ 分别为权限被继承的角色范围和隐式授权的权限范围，且均符合授权约束或预期，即不会出现非预期的权限授予。

(2)若 (r_1,r_2) 为互斥角色约束，r_3 为支配 r_2 的任一角色，即 $r_3 \succ r_2$，若 $(u,r_1) \in UA$，则 $(u,r_2) \notin UA$ 且 $(u,r_3) \notin UA$，即权限扩散不会导致违背职责分离约束产生。

定义 6(管理权限委托可控) 满足以下条件时，称授权管理满足管理权限委托可控。

任意用户、角色、资源及其访问权限都由唯一管理者负责管理，管理权限不会发生非预期的更改，管理权限的使用应符合授权模型安全约束的限制。

对于角色授权，该条件要求资源的管理遵循“谁的资源谁负责的原则”，保证任何资源及其访问权限有且仅有一个管理员进行管理；对于用户授权部分，由系统管理员持有对用户、角色及用户-角色分配关系等的管理源权限，并可将其管理权限委托给具有系统管理员角色的下级管理角色的管理员，且权限委托后，委托者的管理权限暂时回收，仅当委托权限得到撤销后委托者的管理权限恢复，从而保证每个对象仅有一个管理员管理，便于授权责任认定。

委托过程中，委托的权限及其委托深度均应得到模型安全约束的限制，如应委托管理的对象、委托的权限、是否允许再次委托、委托深度等，应明确接受委托权限的受托者的可管理范围及具体权限，从而对管理者可执行的权限和管理对象进行有效控制，避免权限滥用和泄漏。

定义 7(满足职责分离) 当满足以下条件时，称授权管理支持并满足职责分离要求。

某状态 s 下的用户-角色分配关系满足互斥角色约束 C 即 $safe_C(s)$ 时，系统一定满足职责分离策略 E 即 $safe_E(s)$。该授权管理支持并满足职责分离的要求可形式化表示为 $safe_C(s) \rightarrow safe_E(s)$。

由于负责角色权限分配的授权管理员熟知角色层次关系和权限层次关系，该条件要求角色权限分配过程能够为角色合理分配资源的访问权限，使得用户角色分配过程只需满足互斥角色约束，即能够保证系统一定满足职责分离策略，从而确保资源得到安全的访问。

作为 RBAC 支持的一个重要安全原则，职责分离对授权管理的安全性起着重要作用，能否支持并满足职责分离策略是验证和衡量授权管理安全性的重要指标之一。

4.3 可用性准则

可用性是确保授权管理操作有效执行的又一重要指标，强调了访问权限的可用性和资源访问权限可被分配的性质。

定义 8(资源访问权限的可用性) 当满足以下条件时，称授权管理满足权限不会被非预期撤销要求。

假设 p 是由有效资源和资源操作构成的权限，则 $(\exists r \in R, u \in U)((r,p) \in PA \wedge (u,r) \in UA)$ 成立，即对于任一有效权限 p，均可授予角色 r，并被拥有角色 r 的所有用户使用。

该条件要求所有由有效资源和资源操作构成的权限和被授予的访问权限都是可用的。由于权限 p 是有效的，可被授予角色 r，则拥有角色 r 的任一用户都能使用 p，应确保这些用户都能够在需要时正常使用权限 p，且不会随着授权管理操作的执行产生非预期的变更、撤销或失效。

5 安全准则分析

授权管理安全准则用于评价基于 RBAC 的授权管理过程的安全性，其整体结构如图 9 所示。

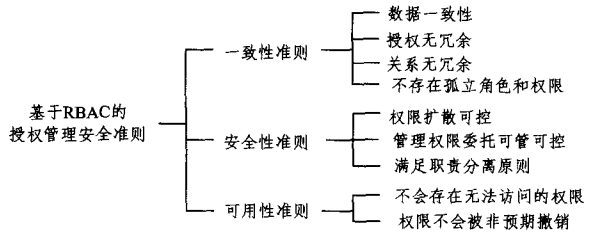

图 9 基于 RBAC 的授权管理安全准则

从图 9 可知，基于 RBAC 的授权管理安全准则包括一致性准则、安全性准则和可用性准则，构成了验证基于 RBAC 的授权管理模型安全性的标准和依据。这些安全准则能够准确地支持现有研究中广泛采用的 Li Ninghui 教授提出的 5 个 RBAC 安全特性：简单安全特性、简单可用性、限定安全性、活性和包容性。

其中，数据一致性确保了用户通过角色获得的权限是有效的，不会出现被意外拒绝访问的情形，避免了授权数据不一致带来的权限泄漏问题，与 RBAC 安全特性中的简单安全特性一致；授权无冗余和关系无冗余要求用户和角色得到的权限及角色层次关系、资源层次关系、资源操作蕴含关系和权限蕴含关系之间不会发生重叠、交叉或覆盖现象，使得撤销权限操作能够正确、有效地执行；不存在孤立角色和权限保证授权管理对象是可管理的，不会出现冗余的对象信息，保证了每个有效资源都是可被访问的，同时每个有效权限都是可被用户使用的，与活性和简单可用性保持一致；权限扩散可控确保了授权管理过程中不会发生非预期权限授予现象和违背职责分离原则的情况，使得实际的扩散权限与管理操作执行的预期相一致，避免了权限不受控制地扩散从而导致权限泄漏，与简单安全特性相一致；管理权限委托可管可控要求管理权限的委托和回收与操作预期相一致，确保不会发生非预期的更改，对管理者可执行的权限和管理对象进行了有效控制，避免权限滥用和权限泄漏，与简单安全特性保持一致；满足职责分离原则要求角色权限分配过程能够为角色合理分配资源的访问权限，使得用户角色分配过程只需满足互斥角色约束即能够保证系统一定满足职责分离策略，确保了用户不会同时拥有互斥角色从而获得冲突权限，与限定安全特性一致；不会存在无法访问的权限和权限不会被非法预期撤销均属于资源权限的可用性准则，确保由有效资源和资源操作构成的权限都可被授予角色进而分配给用户，而任何持有有效权限的用户均可正常使用该权限，不会发生访问被意外拒绝的情况，同时确保了用户正常使用的权限不会由于管理操作错误而造成原本

有效的权限发生非预期减少或无效情况，避免管理操作不当导致权限不可用情形，从正确性和一致性角度确保授予用户的访问权限总是有效可用的；同时，资源访问权限的可用性准则确保任何持有角色 r 的用户均可使用 r 对应的权限访问指定资源，在保证访问权限的可用性的同时，还与包容性保持一致，能够为授权管理的包容性提供有效性保障。

分析可知，数据一致性、权限扩散可控和管理权限委托可管可控为简单安全性提供支撑；不存在孤立角色和权限、资源权限的可用性为简单可用性提供支撑；满足职责分离原则为限定安全性提供支撑；不存在孤立角色和权限为活性提供支撑；权限扩散可控和资源权限的可用性为包容性提供支撑。因此，基于 RBAC 的授权管理安全准则能够全面支持现有广泛采用的 Li Ninghui 教授提出的 RBAC 安全特性，进而为基于 RBAC 的授权管理的安全性提供判定标准、依据和有效保障。

结束语 RBAC 模型本身的安全是授权管理正确、有效和安全执行的关键，授权管理安全准则是验证模型安全的基础。从研究授权管理的安全性入手，分析了与基于 RBAC 的授权管理相关的安全特性，分析给出了基于 RBAC 的授权管理安全需求，从一致性、安全性和可用性 3 个方面研究了基于 RBAC 的授权管理安全准则，期望通过该安全准则，为基于 RBAC 的授权管理模型的执行过程提供一种安全性评估标准。分析结果表明，基于 RBAC 的授权管理安全准则能够全面支持现有广泛采用的 RBAC 安全特性，可为基于 RBAC 的授权管理的安全性提供判定标准、依据和有效保障。

授权管理安全准则研究对推动基于 RBAC 的授权管理模型的安全性分析和验证具有重要意义。然而，授权管理安全准则研究仅仅是模型安全判定的前提，后续研究中还需要对安全准则的正确性和有效性进行验证，并利用该准则验证现有基于 RBAC 的授权管理模型是否安全以验证其可行性。

参 考 文 献

[1] Ferraiolo D, Kuhn D R. Role-Based access control[C]// Proceedings of the 15th National Computer Security Conference. 1992: 554-563

[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, Guirila 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] Munawer Q, Sandhu R S. Simulation of the augmented typed access matrix model (ATAM) using roles[C]// Proceedings of INFOSECU99 International Conference on Information and Security. 1999

[5] Crampton J. Authorizations and antichains[D]. Thesis, Birbeck College, University of London, UK, 2002

[6] Koch M, Mancini L V, Parisi-Presicce F. Decidability of safety in graph based models for access control[C]// Proceedings of the 7th European Symposiumon Research in Computer Security. 2002: 229-243

[7] Li N H, Mitchell J C, Winsborough W H. Beyond proof-of-compliance: Security analysis in trust management[J]. Journal of the ACM, 2005, 52(3): 474-514

[8] Li N, Tripunitara M. Security analysis in role based access control[J]. ACM Transactions on Information and System Security, 2006, 9(4): 391-420

[9] Sasturkar A, Yang P, Stoller S D, et al. Policy analysis for administrative role based access control[C]// Proceedings of the 19th IEEE Workshop on Computer Security Foundations. Washington: IEEE Computer Society, 2006: 124-138

[10] Habib M A, Abbas Q. Mutually exclusive permissions in RBAC [J]. Int. J. Internet Technology and Secured Transactions, 2012, 4(2/3): 207-220

[11] Ferrara A L, Madhusudan P, Parlato G. Security Analysis of Role-based Access Control through Program Verification[C]// Proceedings of 2012 IEEE 25TH Computer Security Foundations Symposium. 2012: 113-125

[12] Yang Ping, Gofman M, Yang Zi-jiang. Policy Analysis for Administrative Role Based Access Control without Separate Administration[C]// Wang L, Shafiq B, eds. IFIP International Federation for Information Processing 2013 (DBSec 2013). LNCS 7964, 2013: 49-64

[13] Liu Xiao-fan, Alechina N, Logan B. Expressing User Access Authorization Exceptions in Conventional Role-Based Access Control[C]// Deng R H, Feng T, eds. Springer-Verlag Berlin Heidelberg 2013(ISPEC 2013). LNCS 7863, 2013: 233-247

[14] 王婷. 面向授权管理的资源管理模型研究[D]. 郑州：信息工程大学，2011

[15] Harrison M A, Ruzzo W L, Ullman J D. Protection in operation systems[J]. Communications of the ACM, 1976, 19(8): 461-471

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

[17] 徐璐. 基于安全标记的 Web 应用访问控制技术研究[D]. 郑州：信息工程大学，2009

(上接第 101 页)

[15] Kolter J, Schillinger R, Pernul G. A Privacy-Enhanced Attribute-Based Access Control System[C]// Data and Applications Security 2007. LNCS 4602, 2007: 129-143

[16] 葛强，沈国华，黄志球，等. Web 服务中支持本体推理的隐私保护研究[J]. 计算机科学与探讨，2013(6): 536-544

[17] 黄凤. 基于描述逻辑的访问控制策略冲突检测方法研究[D]. 南京：南京航空航天大学，2010

[18] Yagüe M, Mana A, Lopez L, et al. Applying the Semantic Web Layers to Access Control[C]// Proc. of the DEXA2003 Workshop on Web Semantics (Webs 2003). Prague, Czech Republic, September 2003

[19] Shen Hai-bo. A Semantic-Aware Attribute-Based Access Control Model for Web Services[C]// ICA3PP 2009. LNCS 5574, 2009: 693-703

[20] Cirio L, Cruz I F, Tamassia R. A Role and Attribute Based Access Control System Using Semantic Web Technologies[C]// OTM 2007 Ws. Part II, LNCS 4806, 2007: 1256-1266

[21] Zha D, Jing Ji-wu, Liu Peng, et al. Proactive Identification and Prevention of Unexpected Future Rule Conflicts in Attribute Based Access Control[C]// ICCSA 2010. Part IV, LNCS 6019, 2010: 468-481

[22] Berners-Lee T, Hall W, James A, et al. Weitzner: A framework for Web science[J]. Foundations and Trends in Web Science, 2006, 1(1): 1-130