数据库访问控制研究综述*)

赵宝献　秦小麟
(南京航空航天大学信息科学与技术学院　南京210016)

摘　要　信息技术的迅速发展使数据库面临的安全更加复杂,访问控制(Access Control)是数据库安全领域的一个重要部分。本文首先回顾了传统的数据库访问控制各自存在的缺点,并总结了传统访问控制的不足之处,由此引出了现代访问控制方法——使用控制(Usage Control,UCON),在此基础上总结了数据库访问控制技术的发展现状,并指出了在此方面进行研究的难点和需要解决的关键问题,并对今后发展的趋势进行了展望。

关键词　数据库安全,访问控制,使用控制

A Survey on the Database Access Controls

ZHAO Bao-Xian　QIN Xiao-Lin
(Information Science and Technology Institute,Nanjing University of Aeronautics and Astronautics,Nanjing 210016)

Abstract　With the rapid development of information and technology,database faces more serious security situation. Research in the access controls has been an important part of the area of the database. Firstly,we review traditional access controls and analysis shortcomings of them. Then,the paper summaries disadvantages of traditional access controls and introduces modern access control---usage control. Based on what we discuss,the paper gives a view of the development of the database access control. In conclusion. it points out the difficulties of research and the existing problems that must be solved. Finally,the future direction in this field is discussed.

Keywords　Database security,Access control,Usage control

1　介绍

在20世纪60年代到70年代期间,自主决策访问、强制访问技术受到了挑战,于是便开始了访问控制的研究工作。对于数据库的访问控制研究工作,到目前为止,已经达到一个非常成熟的阶段。其中已经把早期的访问控制方法以及在20世纪90年代形成的角色访问控制方法(Role-based Access Control)[4,8,12,13]归入传统的访问控制方法。随着数字信息时代的到来,传统的访问控制方法已经适应不了数字化环境下的复杂安全要求,这就需要新的访问控制技术来适应这一需求。于是在原有的基础上形成了现代的访问控制技术----使用控制技术(UCON)[9~11]。

本文首先回顾了传统访问控制方法,并分析了各自的缺点。在分析传统访问控制的基础上,总结了传统访问控制的不足之处。由此引出了现代访问控制方法----使用控制方法,简单介绍了使用控制方法的适用范围以及它的核心ABC(Authorizations,oBligations,and Conditions)[11,26]模型,在此基础上总结了数据库访问控制技术的发展现状。在结论部分,指出了在此方面进行研究的难点和需要解决的关键问题,最后对今后发展的趋势进行了展望。

2　传统访问控制的回顾和分析

传统的访问控制包括:自主决策访问控制(Discretionary Access Control,DAC)[1]和强制访问控制(Mandatory Access Control,MAC)[1,2],以及在它们基础上形成的适应性强制访问控制(Adapted Mandatory Access Control,AMAC)。对AMAC的进一步研究和改造的角色访问控制(Roled-based Access Control,RBAC)[4,8]方法也是一种传统的访问控制。自主决策访问控制(DAC)定义了一套规则,通过这套规则安全主体根据它们的判断,来决定创建(Create),删除(Delete)安全客体,以及授权给其他主体。强制访问控制(MAC)通过控制主体和客体之间的信息流来控制对数据的访问,虽然强制访问控制很有效,但是存在缺陷。其中用来克服强制保护系统某些限制的方法就是角色访问控制(RBAC),该方法重点在安全数据库的设计上。角色访问控制(RBAC)通常被认为是对传统的自主访问和强制访问控制(DAC和MAC)的一个很有前途的两者选一,该模型是一种中性策略。

2.1　自主访问控制(DAC)

自主访问控制是操作系统和DBMS系统的基础,至今已经研究了很长时间。自主决策访问控制一个重要的属性是能支持委托授权规则。大部分系统中的DAC存取控制是用访问控制矩阵(Access Control Matrix)来实现的。该方法可控制主体对客体的直接访问,但是不能控制间接访问。访问控制矩阵一般比较大,通常使用访问控制表(ACL)、容量表(CL)来实现,其中授权关系是前两者的集合,利用关系访问矩阵,每个关系表示一个主体对客体的访问权限,并利用数据库存放访问矩阵。

自主访问控制被用在大部分商业DBMS产品中,一般都以数据库视图的概念为基础。笔者通过总结发现,自主访问控制存在以下的缺陷:

1.安全策略的实行问题:DAC是建立在信息拥有权的概念上的。DAC系统把信息拥有权分配给数据项的创建者,并且允许拥有者(主体)授权存取给其他用户。这就造成了这样一个缺点:企业实行安全需求的负担是在于用户自身的职责,如果没有很高的开销,企业不能控制安全策略。

2.层叠授权问题[21]:如果两个或者多个主体同时把某个

*)基金项目:航空科学基金(编号:02F52033)资助项目。赵宝献　硕士研究生,主要研究方向为数据库安全。秦小麟　教授,博士生导师,主要研究方向为安全数据库、空间数据库、时空数据库、GIS等。

存取模式授权给其他用户(或者从其它用户授权),有可能导致层叠取消授权链。

3. 不能防止特洛伊木马攻击(Trojan Horse Attack)

4. 更新导致的完整性问题:由于并不是所有的数据通过视图可以更新,如果透过包含在数据的数据进行更新数据有可能导致数据的完整性矛盾。

2.2 强制访问控制(MAC)

DAC 涉及到定义、建模以及对属性的访问实施,强制访问控制还涉及到系统中信息流的处理。在强制访问控制中涉及到安全客体和用一个安全标记表示的指定了某个安全级别的安全主体。在强制访问控制中预先定义了安全主体的安全级别以及安全客体(信息)的敏感程度(安全级别)。用户访问必须遵守安全政策划分的安全级别的设定以及有关访问权限的设定,来访问信息。

尽管比自主访问控制(DAC)有更严格的约束,但同时强制访问控制技术需要一些外延的应用来有效地支持对数据库的访问控制。实际上,强制访问控制中存在如下几点问题:

1. 安全客体的粒度问题 至今对于标记数据的粒度没有统一的标准。准确的标记是很有必要的,否则会导致标记指定的不一致性和不完整性。

2. 缺少自动安全标志技术[1]:数据库中通常包含大量的数据集合、服务用户,并且标记数据在许多应用场合是不能够获取的。因此手动安全标记是很有必要的,否则会导致大数据库中无止境进程的发生。因此,支持自动安全标志的技术是很有必要的,顾名思义,就是多级数据库中的指导方针和设计帮助,以及帮助决定相关安全客体的工具,以及参考安全级别和敏感程度的工具。

3. 不支持 N 人访问规则[27]。

4. 执行完整性操作非常复杂。对于强制访问控制中数据完整性的实现和分析相当复杂,具体可以参看文[2]。

2.3 适应性强制访问控制(AMAC)

适应性强制访问控制可以更好地适应于一般目的的数据,处理实践和为包含敏感信息的数据库提供一个设计框架,这些就是适应性强制控制的主要目的。为了克服基于强制控制的限制,AMAC 具有好几个设计特色,这些特色可以帮助一个数据库设计者在设计一个包含敏感信息的数据时实现不同的操作[27]。

但是 AMAC 对于授权和收权没有特别深入的研究,不适合于商业用途。这种强制访问控制实现的工作量比较大(具体如何实现可以参看文[27]),管理不方便。AMAC 中角色只是适合集中数据库,对于分布式数据没有做出定义和研究。AMAC 只是从传统的访问控制方法到最近 RBAC 访问控制方法的一个过度模型。

2.4 角色访问控制(RBAC)

角色访问控制(RBAC)通常被认为是对传统的自主访问和强制访问控制(DAC 和 MAC)的一个很有前途的两者选一,即它是一种中性策略,近些年的研究已经使 RABC 日趋成熟,在 RABC 模型中可以表示 DAC 和 MAC 模型。RBAC 和以前的访问控制相比,它通过增加角色(Role)和许可(Permission),方便了管理。RBAC 模型中一般的体系是 RBAC96,该模型是 Sandhu 等人提出的[12,13]。

RBAC 一个最重要的特色就是它自身是一个中性策略。RBAC 是一个结合策略的方法而不是具体化某一个特殊的安全策略的方法。在一个具体系统中策略的实施实际上是精确配置和直接被系统拥有者控制的不同 RBAC 组成部分交互作用的纯粹结果。此外,访问控制策略可以在系统生命周期中不断进化,通常在大的系统中一定要这样做。这种可以根据企业中变化的需要来修改策略的能力是 RBAC 的一个重要优点。

通过对文[4,12~14,17,18,25]的分析,总结出存在以下的缺点和改进之处:

1. 这种方法缺少信息模型的概念和表达[18](信息模型就是能够获得信息使用组织的和分布式方面)。

2. 到目前为止角色机制里面的委托授权(Delegation)没有研究。计算机系统中的委托授权可能是人对人,人对机器,机器-机器,甚至机器对人。这些类型的委托授权已经在安全领域里引起了很大的关注,然而,人对人的委托授权至今还没有被系统地分析。

3. RBAC 在文[4]中为几个重要的安全规则提供了支持,例如支持最小权力(Least Privilege)、权力提取(Privilege Abstraction)以及职责分离,但是没有详细指出如何实现这些目标。

4. RBAC 最大的优点就是方便许可的管理,但是如何实现 RBAC 对自身的管理,至今还处于不断研究完善中。到目前为止 Sandhu 等人在文[25]中定义的管理 RBAC 模型(ARBAC97)为这个方向的研究提供了一个很大的进展。但是 ARBA97是一个低级模型,该模型建立比较单一乏味,在将来,有必要找出更多 RBAC 管理的抽象模型。

5. 在 RBAC[12,25]模型中,很难精确地识别许可的属性。因为 RBAC 模型是一个中性策略,所以,许可的属性是无限制的。将 RBAC 实施到一个具体的系统中的时候,许可的解释是实施中最重要的步骤。

以上我们讨论了传统的访问控制。这些传统的访问控制只是对封闭世界的敏感信息进行访问控制[10]。对于现代高速发展的信息时代,我们不难看出它们存在下面的问题。

3 传统访问控制技术存在的问题

传统访问控制,甚至可信管理(Trust Management)一个共同点就是根据主体属性和客体属性来进行授权操作[11]。换句话来说,就是在传统的存取控制中,是由主体属性、对象属性以及要求权利来决定授权的。其中属性包括一致性(Identity)、容量(Capability),或者主体(或者客体)的属性。例如,在 MAC 中,主体的安全级标记被作为主体的属性,客体的敏感度标记作为客体的属性。然后,在授权过程中,对于请求访问的权利(例如,读,写)来考虑这些标记的域,最后返回允许还是不允许。类似地,在 DAC 中,访问控制表(ACL)可以看作客体的属性,容量表(CL)看作主体的属性。

我们可以看出传统的访问控制主要集中在控制授权的研究上,虽然可以应用到好多应用场合,但是今天的数字信息系统需要的不仅仅是级别授权。在现代数字信息系统中,使用决定是以请求行动的实现为基础的,而不是主体属性和客体属性的存在为基础的。这一决定因素称之为职责(Obligation,B)[9],此外还需要授权(Authorization,A)来适合现代存取控制应用场合。在处理某个请求时,系统在做出使用决定时,需要核对当前的环境或者系统状态。这个决定因素称之为条件(Condition,C)[9],在现代存取控制技术中同时集合了授权(A),职责(B)和条件(C)。

除了上面的3个决定性因素之外,现代信息系统还需要其他的两个重要的属性:连续性(Continuity)和易变性(Mutability)[11]。在传统的访问控制中,是假设在访问允许前授权的。现代访问控制可以通过连续性保证在访问前、访问中、访问后都可以进行授权和收权。

在传统的访问控制领域里，很少讨论到属性的易变性。属性仅仅能被管理员作修改。现代访问控制技术可通过属性的易变性来保证属性可以在访问中根据情况进行对属性的修改。拥有了连续性和易变性，现代访问控制技术更加丰富了访问控制的动作和范围。

尽管这些问题在一些访问控制的文献中早有涉及，但是它们的焦点局限于具体所涉及的问题，缺少对所讨论问题的全面理解。使用控制(Usage Control，UCON)[9~11]概念的形成是为了在一个简单的构架下解决这些不同的问题，克服这些缺点的。Sandhu 在文[9]中首先提出 UCON 的概念，并在文[11]中提供了 UCON 的框架。

4 访问控制新方法——UCON

在 UCON 中，把传统的访问控制扩展到现代访问控制中，并具有授权、职责和条件的数字权力管理，还包括一致性和易变性。

下面我们将重点介绍一下这种新的访问控制方法--UCON。

4.1 UCON 的范围

使用控制主要集中在预防(例如，水印技术)上，尽管在 UCON 框架里也实现了探测和响应机制。

在使用控制中，仅仅数字信息资源是对象客体，这样可以对数字资源进行连续的保护而不管系统环境、访问方法或者地点。因此，不像其他的资源，信息资源涉及到唯一问题，例如隐私问题。

4.2 UCON 的目的

使用控制的目标[9]就是为访问控制提供一个新的智能基础。在早期的访问矩阵研究中，20世纪30年代的旧框架不再能适合研究者的需求，已经在不同的方向被扩展了。这些结果都是没有根本智能结合表面扩展的过剩产物。因此，名词使用控制(Usage Control)表达了更广阔的观点。使用控制全面集合了传统访问控制、可信管理以及数字管理管理[11]。使用控制用一个简单的框架系统统一了这些领域，文[26]给出了 UCON 的覆盖范围以及它和其他研究领域的关系。

4.3 UCON 的模型

ABC 模型(Authorizations，oBligations，and Conditions)[11]是 UCON 的核心模型。之所以称之为核心模型，是因为它阐述了使用控制中最基本的问题，不涉及到管理、委托授权，以及其他后期工作中的重要问题。使用控制(UCON)集合了传统的访问控制、可信管理以及数字权力管理，并且超出了它们的范畴。

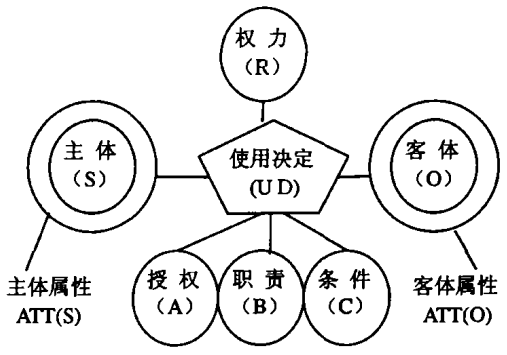

图1 ABC 模型的组成

ABC 模型有8个核心组成部分(如图1)。它们是主体(Subjects，S)，主体属性(Subject Attributes，ATT(S))，客体(Objects，O)，客体属性(Object Attributes，ATT(O))，权力(Right)，授权(Authorizations，A)，职责(Obligations，O)，条件(Conditions，C)。其中职责和条件是最近提出来的[9,11]，用来解决传统访问控制中的缺点。

ABC 模型中一个显著的改革在于主体和客体属性是可以变化的，即易变性(Mutability)。易变属性的引入是 ABC 模型相对于大部分增强访问控制模型建议的一个关键区分点[11]。

ABC 模型通过用一个系统的方法统一了这些不同的领域，为下一代访问控制提供了新思路。

使用控制是一个可以适用这些现代信息安全领域的概念框架，它以系统的方式提供了一个保护数字资源的一般目的，统一标准的框架。UCON 与其说是对传统访问控制、可信管理、或者数字权力管理的替代，而不如说是它集合了这些领域的优点，并且超出了它们的定义和范畴。同时，UCON 可以对数字值进行精细的控制，甚至在对象已经发布出去。

结论和展望 在这篇文章中，我们首先回顾了传统的访问控制方法，并对它们做了进一步的分析。最后我们总结出了它们的缺点，引入了新的访问控制方法--使用控制(UCON)。限于篇幅我们对该方法做了简单介绍，详细介绍可以参看文[9～11]。由此我们对数据库的访问控制方法的研究过程有了一个清晰的了解。

使用控制方法是一个全面的包含传统访问控制和现代访问控制(例如数字权利管理和应用)的一个全新的方法。目前对访问控制方法的研究，只是处于起步阶段，Mason 大学的 Sandhu 等人正在从事这一研究。其中我们介绍的 ABC 模型是他们对使用控制研究的最新成果，但是 ABC 模型只是一个核心模型，其中并没有涉及到管理、委托授权[11]。现今使用控制研究的主要目的只是为分析现有和将要开发的新系统提供一个基本的参考性框架。为了将使用控制使用到现实世界的应用场合，对使用控制工程的研究必须进行。具体来说，必须制定很好的设计决定规则和属性，来引导使用决定策略的分析。在有设计很好的使用控制系统中，可以提高使用控制的易变性。因此，对使用控制实现工程的进一步研究是使用控制技术取得成功的因素之一。

我相信对以上问题的进一步研究将会给使用控制提供一个更容易解决的方法。我们相信使用控制技术将为下一代访问控制方法提供一个牢固的框架基础[11]。

参 考 文 献

1 Sandhu R. Relational Database Access Controls. Handbook of Informantion Secutrity Management(1992-95 Yearbook), Auerbach Publishers, 1994. 145～160

2 Sandhu R. Mandatory Controls For Database Integrity. In: Proc. of the IFIP WG11. 3 Workshop on Database Security, Monterey, Colifornia, Sep. 1989

3 American National Standard for Information Technolology. Role Based Access Control. Information Technology Industry Council (ITI), Draft, Apr. 2003

4 Ferraiolo D F, et al. Proposed NIST Standard for Role-Based Access Control. ACM Transaction on Information and System Security, 2001, 4(3): 224～274

5 Graubart, Richard. On the Need for a Third Form of Access Control. In: Proc. of the 12th National Computing Security Conf. 1989. 296～303

6 Sandhu R, Chen F. The Multilevel Relational (MLR) Data Model. ACM Transactions on Information and System Security, 1998, 1(1): 93～132

7 Sandhu R, Jajodia S. Data and Database Security and Controls. Handbook of Information Security Management, Auerbach Publishers, 1993. 481～499

8 Ferraiolo D F, Cugini J, Kuhn D R. Role Based Access Control: Features and Motivations. In: Computer Security Applications

Conf. 1995
9 Park J, Sandhu R. Towards Usage Control Models: Beyond Traditional Access Control. SACMAT02, Monterey, Califomia, USA, ACM, 2002
10 Park J, Sandhu R. Originator Control in Usage Contrlol. In: 3rd International Workshop on Policies for Distributed Systems and Networks(Policy02). June 2002
11 Sandhu R, Park J. Usage Control: A Vision for Next Generation Access Control. MMM-ACNS 2003
12 Sandhu R, Coyne E J, Feinstein H L, Youman C E. Role-based access control models. IEEE Computer, 1996, 29(2): 38～47
13 Sandhu R. Rationale for the RBAC96 family of access control models. In: Proc. of the 1st ACM Workshop on Role-Based Access Control. ACM, 1997
14 Barkley J. Comparing Simple Role Based Access Control Models and Access Control Lists. In: Proc. of the Second ACM Workshop on Role-Based Access Control, Nov. 1997. 127～132
15 Park J, Sandhu R, Schifalacqua J. Security Architectures for Controlled Digital Information Dissemination. ACSAC, 2000
16 Sandhu R. Access Control: The Neglected Frontier. ACISP, 1996
17 Chen F, Sandhu R. Constraints for RBAC, ACM RBAC, 1995
18 Thomas R, Sandhu R. Conceptual Foundations for a Model of Task-based Authorizations, CSFW, 1994
19 Sandhu R. Design and Implementation of Multilevel Databases. RADC, 1994
20 Sandhu R, et al. Role-Based Access Control: A Multi-Dimensional View. ACSAC, 1994
21 Thomas R, Sandhu R. Discretionary Access Control in Object-Oriented Databases: Issues and Research Directions. NCSC, 1993
22 Jajodia S, Sandhu R. Toward a Multilevel Secure Relational Data Model. SIGMOD, 1991
23 Sandhu R. Evaluation by Parts of Trusted Database Management Systems. RADC, 1991
24 Sandhu R, Share M. Some Owner-Based Schemes with Dynamic Groups in the Schematic Protection Model. OAKLAND, 1986
25 Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-Based Administration of Roles. ACM Transactions on Information and System Security, 1999, 2(1): 105～135
26 Park J, Sandhu R. The UCONABC Usage Control Model. ACM Transactions on Information and System Security (TISSEC), Feb. 2004
27 Yovits M C. Database Security. Advances in Computers. Academic Press, 1994, 38: 1～74

(上接第87页)

类标识属性，其仅供算法结果分析。表1和图1是各数据集中攻击类型分布情况。

表1 实验数据集结构

	实例数	正常实例数	入侵实例数	攻击类型数据	分类攻击数
数据集1	2100	2000	100	21	4
数据集2	2100	2000	100	11	3
数据集3	2100	2000	100	13	4
数据集4	2100	2000	100	8	2
数据集5	2100	2000	100	13	4

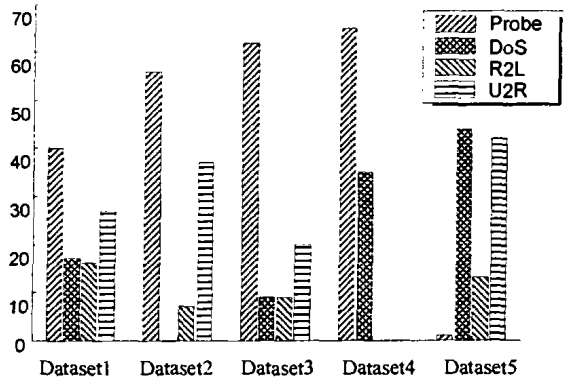

图1 实验数据集中攻击类型分布

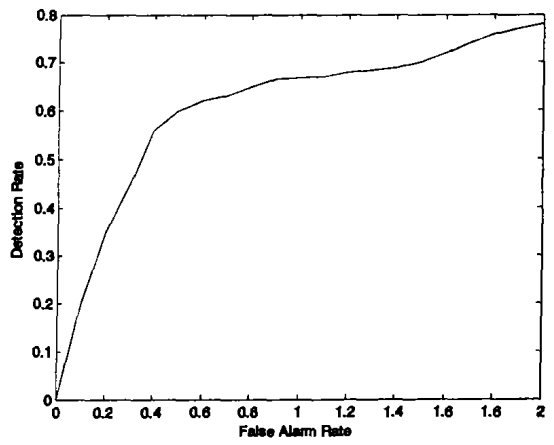

图2 NIDBFCM 检测率和误检测率的相对曲线

针对以上数据集，选用实验平台 Windows2000，Matlab6.5语言编程环境，Intel Celeron 1.70GHz CPU，256MB 内存。为评价入侵检测算法性能使用两个指标：检测率 DR(Detection Rate)和误检率 FR(False Alarm Rate)。检测率 DR 是被系统检测到的入侵实例数目与检测数据集中总的入侵实例数目之比；误检率 FR 则为被误判为入侵的正常实例数目与总的正常实例数目之比。这两项性能指标能充分反映算法的入侵检测能力。最好的入侵检测系统应该使 DR 尽可能的大，而 FR 则尽可能的小。图2是上述5组实例数据的平均检测结果，在隶属度改变的情况下，检测率提高的情况下，误检率也会提高。

从图2可知最好性能当 FR＝1%时，DR＝69%，这充分表明算法对于未知入侵行为检测的可行性和有效性，与 Portnoy 提出的方法相比，在一定程度上提高了检测率，降低了误检率。

结束语 本文分析了聚类技术及其在入侵检测中的应用，提出以 FCM 进行入侵检测，分析了检测过程，并用 KDD-99实验数据集进行仿真实验，其结果表明该算法提高了检测的效率，算法是可行的、有效的。

参 考 文 献

1 Wenke L. A Data Mining Framework for Building Intrusion Detection Models. In IEEE Symposium on Security and Privacy, 1999
2 Lee W, Stolfo S J, Mok K W. Mining in a data-flow environment: experience in intrusion detection. submitted for publication, 1999
3 Portnoy L, Eskin E, Stolfo S J. Intrusion detection with unlabeled data using clustering. In: Proc. of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001). Philadelphia: ACM Press, 2001(11)
4 Li Xiangyang. Clustering and Classification Algorithm for Computer Intrusion Detection: [PhD.]. Arizona State University, 2001. 12
5 Equihua M. Fuzzy clustering of ecological data J. Ecol, 1990, 78: 561～567
6 http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html