●周朴雄

访问控制在数据安全系统中的应用*

摘 要 访问控制是指控制用户访问文件、目录、端口甚至协议的方法。在数据库安全系统中，访问控制主要有 4 种技术得以运用：防火墙技术、身份鉴别与认证技术、存取权限控制技术、审计跟踪技术。图 2。表 1。参考文献 5。

关键词 数据库安全系统 访问控制 身份鉴别认证 审计跟踪
分类号 G250.74

ABSTRACT Access control is the method for the control of user to access file, directory, port, or even protocol. In a data security system, there are four techniques for access control: firewall technique, ID authorization, access privilege control technique and audit tracking technique. 2 figs. 1 tab. 5 refs.

KEY WORDS Data security system. Access control. ID authorization. Audit tracking.
CLASS NUMBER G250.74

1 访问控制在数据库信息安全系统中的重要性

在开放式的信息系统网络中，数据库系统的安全有其自身的敏感性，也有其问题的深层性[1]。不论信息系统如何组织，采取何种结构，如果它不是建立在“可信安全基”上，没有足够的安全性，一旦受到攻击，后果是严重的。本文所论及的数据库系统安全仅指数据库系统中信息的安全问题，而不是系统运行的安全。

由于数据库系统中信息的重要性及共享性，而操作系统对于数据库文件又没有特殊的安全保护措施，数据库系统便成为各种黑客或入侵者攻击或入侵的重点。随着计算机科学技术的发展，特别是计算机的普及、网络的发展、硬件和软件知识的透明度的增强以及计算机使用方法的通用性的提高，数据库系统的安全正受到多方面的威胁，主要有[2]：

(1)软件的保护功能失效造成信息泄漏，如在数据库系统设计上存在缺陷，缺少存取控制机制或破坏了存取控制机制，造成信息泄漏。

(2)非授权用户非法存取、篡改数据。如果数据库管理人员对数据的使用权限不进行严格控制，对哪些人有数据访问权、哪些人有数据修改更新权，缺乏严格的检查控制措施，对用户在计算机上的活动没有进行监督检查，就会导致非授权用户非法存取，合法用户对数据进行篡改等[3]。

(3)授权者制定不正确、不安全的防护策略。

(4)操作者复制和泄漏机密、敏感数据资料。

(5)终端使用者隐瞒自己身份，进行不正确的输入。

数据库中信息资源安全是一项动态的、整体的系统工程。从技术上来说，数据库安全系统由安全的操作系统、防病毒、访问控制、防火墙、入侵检测、网络监控、信息审计、通信加密、安全扫描等多个安全组件组成，一个单独的组件是无法确保数据库系统的安全性的。其中，针对数据库安全访问控制在数据库信息安全系统有其重要性与特殊性。

在数据库中存放大量的数据，它们在重要程度及保密级别上都有所不同；同时这些数据由许多用户所共享，而各用户又有各种不同的职责和权限。因此，必须对不同的用户采用不同的程度访问控制，限制数据库用户，使他们得到的不是整个数据库的数据，而只是一些他们所必需的、与他们的权利相适应的数据。不允许用户访问非授权的数据，并严格控制用户修改数据库中的数据，以免因某个用户在未经许可的情况下修改了数据，而对其他用户的工作造成不良影响[4]。

同时，由于数据库是联机工作的，可以支持多用

* 本文为国家教育部重大项目“网络信息资源组织与开发模式”(2000ZDXM870001)的研究成果之一。

户同时进行存取，采取访问控制措施可以防止由此引起的破坏数据库完整性和安全性行为。

2 访问控制技术

2.1 访问控制技术概述

访问控制(Diserctionary Access Control)是指控制用户访问文件、目录、端口甚至协议的方法。它的实现依赖于系统的权限与许可，包括读许可、写许可、执行许可或者更为细致的权限划分，来保证信息资源不被非法使用或非法访问。它还可以使系统管理用户在网络中的活动，及时发现并拒绝黑客的入侵[5]。

访问控制对所有对象提供了所有用户和组账号的安全信息，访问级别由所制定的访问权限控制。因此，可以允许或禁止用户对任意资源的访问。其审核规则控制系统安全日志记录的事件类型，所以，管理员可以跟踪、获悉哪些用户试图对文件和对象进行特殊访问。审核还可以用于跟踪系统登录尝试、系统关闭和重启动等类似的事件。这些都有助于确认各种破坏安全性的行为，并分析破坏的程度和位置，以便采取相应措施。

2.2 访问控制的主要技术

目前，访问控制技术已经比较成熟，主要是基于传统的主体访问对象的模型。这里主体是指计算机系统的用户，而对象是指系统的信息资源。访问控制一般有以下4种技术。

(1)在内部网与外部网之间设置防火墙(包括分组过滤防火墙与应用代理防火墙等)，通过隔离内外网来实现访问控制。但应该强调的是，防火墙只能防止外部黑客的攻击，而不能防止内部黑客的攻击，并且只能进行粗粒度的访问控制，所以，防火墙只是整体安全防护体系的一个重要组成部分，而不是全部。必须将防火墙的安全保护融合到系统的整体安全策略中，才能实现真正的系统安全。

(2)身份鉴别与验证。身份鉴别是在允许用户进入系统，开始任何活动时判断他是谁。验证是使用保护机制进一步断定其身份的真伪。口令系统是身份鉴别与验证的关键。其传输和处理过程是，用户在远程终端上输入口令，运程终端上的一次性口令模块根据输入口令生成随机密钥，网络将一次性密钥传输给原系统(远程服务器)，原系统中的口令与密钥进行匹配运算并返回运算结果，最后运程终端上的一次性口令模块验证返回运算结果，并通知用户是否可以进入系统。口令系统存在的问题是，口令容易被窃取或破译。

(3)权限控制技术。访问权限控制是指对合法用户进行文件或数据操作权限的限制。这种权限主要包括对信息资源的读、写、删、改、拷贝、执行等。对于多级安全的系统，要把主体与客体分割为不同的保密层次。一个主体可读一个客体，仅当主体的安全级高于或等于客体的安全级；一个主体可写一个客体，仅当主体的安全级低于或等于客体的安全级。为实现以上原则，还需要身份识别和验证配合。

(4)审计跟踪技术。计算机网络应有详细的系统日志，记录每个用户每次活动(访问时间和访问的数据、程序、设备等)，以及系统出错信息和配置修改信息。审计是记录用户使用计算机网络系统进行所有活动的过程；跟踪是对发现的侵犯行为实施监控，掌握有力证据，并及时阻断攻击的行动。审计跟踪是一种事后追查手段，是提高系统安全性保密性的重要工具。

在数据库安全系统中的访问控制应该根据系统的实际情况，综合采用这4种技术，并与一定的安全策略和模型结合起来，才能最大程度地保证数据库系统的信息安全。

3 访问控制技术在数据库安全系统的运用

数据库系统的访问控制，应根据不同的系统需求，采用不同的控制力度。比如，保密部门的数据库系统就应该比商品信息系统的访问控制力度要强。这就涉及到一定数据库系统的访问控制策略的制定和模型的生成。

3.1 数据库系统的访问控制策略

由于数据库系统安全的特殊性，在对其进行访问控制时，也应采用一些特殊的安全策略，来指导如何组织、管理、保护和处理敏感信息。针对数据库系统的访问控制应考虑使用以下几种策略。

(1)知需策略。知需策略是指如果需要读写数据对象的某个集合，就只让用户得到其相应权限的信息，其余的信息一律不给。这是因为对用户权利

进行适当的限制,就可以减少泄密和破坏数据库完整的可能性。如果安全控制设在关系级,则一旦用户存取关系,他就可以存取该关系中的所有元组的所有属性。如果控制设在属性级,则用户只能存取该属性。这种策略适用于高级机密部门。

(2)最大共享策略。这种策略与知需策略相反,是使数据库中尽可能多的信息能在最大程度上共享,但这并不意味着每个用户能存取数据库中的所有信息,而是除了需要保护的那部分数据之外的数据。这种策略适用于一般的商用信息处理环境,其中数据共享是数据库运用的重要目标。

(3)按实际要求决定颗粒大小策略。在数据库中,可按要求将数据库中的项分成大小不同的颗粒,颗粒越小,安全级别就越高。通常,要根据实际要求决定颗粒大小尺寸。

(4)开系统和闭系统控制策略。开系统是指用户对数据拥有所有的存取权,除非明确禁止一些项目的存取。这种方式支持数据共享,但当无意删去某规则时,会导致数据的共享性扩大而发生泄密问题。闭系统是指对数据库中的访问都隐含为禁止的,只允许用户对明确授权的项目进行存取,它可以用于使用知需策略的系统。这两种系统按不同要求控制存取,从安全保密角度看,由于闭系统的缺省规则是限制存取,所以闭系统要可靠得多。

一个数据系统究竟使用哪些访问控制策略,应该与该数据库系统的机密程度、使用目标以及实际要求结合起来。对于机密程度不高,以数据共享为主要目标的数据库系统来说,使用开系统和最大共享策略为好;但对于机密程度高,如军事或保密系统的数据库,则应采用闭系统和知需策略。

3.2 数据库系统中的访问控制模型

不管数据库系统中采用哪种访问控制策略,都需与一定的安全模型结合起来,才能准确地表示出安全策略。可以说,安全模型是安全策略的具体化,同时它又作为一种结构指导数据库安全系统的设计。

数据库系统的访问控制模型是基于主体对客体的访问控制。它由3部分组成:主体集合、客体集合和一组定义主体存取客体的操作规则的集合。主体是要求存取数据库的用户、用户组,用S来表示;客体是指要求保护的数据对象,用O表示;存取操作是诸如读、写、更新等操作,通常用t来表示;数据库的所有存取控制规则通常用一个矩阵来表示,称为访问矩阵模型。它把系统的安全状态表示成一个矩形阵列,其中的行为主体S_1、S_2、…S_m,列为客体O_1、O_2、…、O_n,矩阵元素$aij=P(Si,Oj)$,表示主体S_i允许对客体O_j所作的存取操作t,如图1所示。

$$A=\begin{bmatrix} a_{10} & a_{11} & \cdots & a_{1n} \\ a_{20} & a_{21} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m0} & a_{m1} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_m \end{bmatrix} = [O_1 \quad O_2 \quad \cdots \quad O_n]$$

图1 访问矩阵模型

例如,在表1表示了3个用户A、B、C对4个数据对象R_1,R_2,R_3,R_4进行存取控制的规则。其中,用户B可以修改R_1,对R_2可读,对R_3可以删除,对R_4不能进行任何操作。

表1 用户授权表

数据对象	R_1	R_2	R_3	R_4
用户A	ALL	ALL	ALL	ALL
用户B	READ	—	READ	—
用户C	WRITE	READ	DELETE	—

注:"ALL"表示各种存取,如读、写、修改;"—"表示不能进行任何存取。

如果将存取操作t与前面讨论过的安全访问控制策略联系起来,就演变成一条存取规则,可将该规则表示为一个四元组(S、O、T、P),其中P是该存取规则的谓词表示,当它所表示的条件成立时,即对谓词P进行求值,当P满足要求时,允许主体S对客体O进行T类型的存取。存取控制不仅规定存取规则,而且还包括一个验证过程,所有的存取请求(S、O、T、P')都要经过验证过程进行认可,以保证所有对数据的存取都满足存取规则。

3.3 访问控制在数据库安全系统中的实现方案

根据访问控制在数据安全系统中的策略和模型,笔者提出其具体的实现方案(如图2所示)。在该方案里,访问控制主要有4种技术得以运用。它们分别是防火墙技术、身份鉴别与认证技术、存取权限控制技术、审计跟踪技术。

防火墙是数据库安全系统的第一层访问控制,

是用户进出数据库系统的大门,通过它可以屏蔽数据库系统,使外部的非法用户无法进入数据库系统;它自身也可以时时判断和过滤来自外部网络的不良数据包括黑客的攻击企图;还可以时时响应来自数据库系统内部网络其他子系统的阻断请求,对来自外部网络的攻击行为进行阻断;它还对用户的进出进行记录,并与审计跟踪模块进行沟通。

虽然防火墙在一定程度上可以部分地控制非法用户进入数据库系统,但还是有一些外部非法用户采用欺骗等手段进入,或者内部用户冒充管理员而权利得到提升,这些都会对数据库系统的安全造成威胁,所以要对用户进行身份鉴别与认证。数据库管理系统可以要求严格的用户鉴别与认证,要求用户对通行字和日期、时间检查认证。身份鉴别与认证是数据库系统的第二道屏障,进行身份鉴别认证的主要方式是设置口令。对数据库的不同功能块应设置不同口令,并且这些口令应彼此独立。对存取它的用户也应设置不同的口令级别,所形成的口令表应进行加密,并由专人看管。在用户进行身份认证后,应对其进行登记,并交审计跟踪模块。

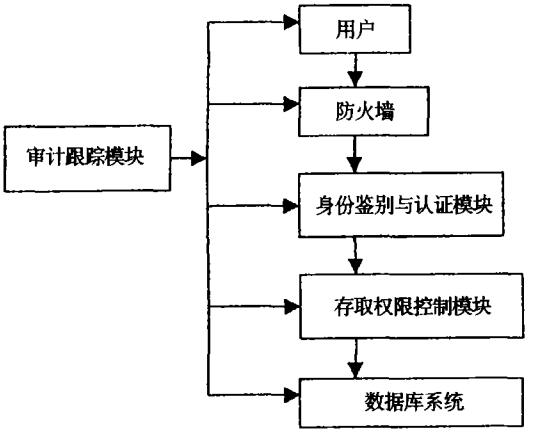

图2 访问控制在数据安全系统中的实现方案

只有经过了防火墙与身份鉴别认证的用户才能进入数据库系统,一旦用户进入系统,它就部分地拥有使用数据库的权利,这时,存取权限控制模块应根据访问控制策略,建立每个用户的存取权限控制表,对其权利进行控制。存取权限控制模块还对用户的每一次存取活动作出记录,交审计跟踪模块。

审计跟踪模块记录对数据库的所有访问(读或写),它可以协助维持数据库的安全性与完整性。审计跟踪模块对进出防火墙、身份认证系统及权限控制模块的活动进行记录与跟踪。它一方面可以帮助在事后发现哪个用户在何时修改过什么值,另一方面,审计记录有利于分析出已给用户什么信息,还可以作为是否要告诉用户更多信息的依据。

以上4个模块互相联动,相互协调,构成一个相对完整的访问控制安全体系,以保障数据库系统的安全。

4 小结

数据库系统的安全维护,不同于一般的信息安全与权益保障,它可以是整个信息安全体系中的重中之重。没有了安全的数据库系统,整个信息安全体系就失去了基础,成了空中楼阁。而访问控制在数据库的安全系统中又显得尤其重要,它可以很好地表达系统的安全策略,同时它在数据库的安全系统中又有其特殊性,这正是本文论述的中心。当然,要维护数据库系统的安全,仅依靠访问控制是不够的,还需要综合运用其他安全技术,比如入侵检测技术、防病毒技术、加解密技术、网络监听技术等。同时还要注意加强数据库系统的安全管理和培养数据库用户的安全意识等。

参考文献

1 [美]匿名著;前导工作室译.网络安全技术内幕.北京:机械工业出版社,1999
2 [美]Derek Atkins等著;严伟,刘小丹,王千祥等译.Internet网络安全专业参考手册.北京:机械工业出版社,1998
3 [美]Terry Escamilla著;吴炎等译.入侵者检测.北京:电子工业出版社,1999
4 [美]Jason Garms等著;郭漫雪,王应波,夏文等译.Windows NT Server 4大全.北京:机械工业出版社,西蒙与舒斯特国际出版公司,1997
5 周朴雄.基于Linux平台的主机入侵检测系统的研究与实现.武汉大学硕士学位论文,2002.5

周朴雄 武汉大学信息管理学院博士研究生。通讯地址:武汉。邮编430072。

(来稿时间:2003-11-04)