计算机科学 1999Vol. 26№. 4

当前流行的 DBMS 安全机制的剖析

The Security Mechanism Parsing of the Popular DBMS Currently

邵佩英　孙淑玲
（中国科技大学研究生院　北京 100039）

Abstract　This paper analyzes the security requirements of database from developing practice for information system. Then parses synthetically the security mechanism of the current popularity RDBMS including Oracle, IBM DB2, Sybase, Informix, Microsoft SQL Server. Through parsing, shows the them common security mechanism and improving for reinforcing the security mechanism of database themselves.

Keywords　Information system, Database, Security, Access control

1. 引言

信息系统的逻辑安全性环节有：存储信息的安全、访问信息的安全和传输信息的安全。数据库和它的管理系统作为信息数据的存储地和处理访问地，应能对信息数据的安全存储和安全访问提供服务，具有安全防范的能力，包括：向合法用户提供可靠的信息服务；拒绝执行不正确的数据操作；拒绝非法用户对数据库的访问；且能跟踪记录，以便为追查责任提供证据和迹象。本文首先分析和总结在信息系统开发实践中对数据库的安全需求，然后针对这些需求，查阅有关资料和实际使用经验，对当前流行的几种关系型数据库管理系统 Oracle, IBM DB2, Syhase, Informix, Microsoft SQL Server 的安全机制进行综合剖析，通过剖析展示它们的共同安全机制，并介绍它们各自为了加强安全机制所作的努力和改进。

2. 数据库安全需求分析

数据库是当前信息系统的基础，数据库的安全是信息系统安全的重要组成部分。数据库安全性受到破坏一般表现为如下三种情形：(1)非法用户对数据库的访问；(2)对数据库执行不正确的修改操作（插入、删除、更新等）；(3)数据库的一致性、完整性被破坏，数据库内的垃圾堆积，使数据库不可用。

由此可见，为了保证数据库的安全性，应满足如下要求：(1)要求数据库具有保密性，以防止非法用户的访问，保护数据库中数据的机密不被泄露；(2)要求数据库具有完整性和一致性，以防止不正确的数据操作或非法用户的恶意攻击；(3)要求数据库具有可用性，以防止和及时修复因软、硬件系统的错误所造成的数据库恶性破坏，并拒绝和清除数据库垃圾；(4)要求能对数据库变化作跟踪记录，以防止否认对数据库的安全责任。

数据库的安全性能由数据库管理系统的内部构件实现。数据库管理系统的加密机制和访问控制机制是数据库保密性的保证，数据库中的数据应是加密存放的；且每当一个用户（或程序）访问一个数据库对象（数据库、表、视图、行、项、存储过程等）时，访问控制机制就会检查该访问的合法性，这是使用访问控制表来实现的。数据库的完整性和一致性由访问控制机制和语义完整性约束联合来保证，每当一个用户对数据库进行修改时，前者检查修改操作的合法性；后者检查被修改数据的语义正确性，这是通过核实语义完整性约束条件来实现的。数据库管理系统的修复子系统用于保证数据库的可用性和正确性，这是使用日志、镜像等来修复和实现的。

3. 当前流行的 DBMS 安全机制的共性

当前流行的数据库管理系统大都是关系型数据库管理系统，包括 Oracle, IBM DB2, Sybase, Informix, Microsoft SQL Server 等。根据对以上几种 RDBMS 资料分析和实际应用总结，尽管它们在具体的做法或命令格式上有所差别，但其实现数据库

安全性的技术和效果在如下几个方面是具有共同性的，

(1)权限(Privilege)和授权(Authorization)。它们大多都支持标准 SQL 中的权限授予语句 GRANT(权限撤消使用 REVOKE 语句)。GRANT 语句的语法如下：

GRANT privilege_list ON object TO user_list [WITH GRANT OPTION]

其中：privilege_list 为被授予的权限列表，权限一般分为对象创建许可权(CREATE)和对象操纵许可权(SELECT，INSERT，DELETE，UPDATE、REFERENCE，EXECUTE 等)；object 为数据库对象名，如表名、视图名、域名、存储过程名等；user_list 为用户或用户组列表，也可是 public 表示对所有用户都授予；[WITH GRANT OPTION]为可选项，如果选择此项，表示该用户或用户组可以将所受予的权限再授予其他用户或用户组，即权限允许扩散。

(2)角色(Roles)，角色可理解为用户的一种特殊的身份，是为特定的用户或用户组定义的一组标准权限，用户权限的获得通过 GRANT 语句。在当前流行的这几种 RDBMS 中，角色及其权限的划分不尽相同，但一般都有系统角色和用户定义角色之分。系统角色是系统预先定义了的，并授予它们管理和控制系统所必需的各种权限，系统角色还可以通过命令来模拟其他角色。用户定义角色是通过命令方式或过程调用方式来定义的(如在 Sybase 中可用 create role 命令或 sp_role 系统存储过程定义)。系统角色在各个 RDBMS 中的名称和职责有所不同，例如：在 IBM DB2 中，数据库管理员(DBA)的任务由三种系统角色(系统管理员、系统维护员、系统控制员)共同完成，他们分别具有系统管理权和数据库管理权、系统维护权、系统控制权，在 Sybase 中，数据库管理员的任务由系统管理员(SA)、系统安全员(SSO)、系统操作员(OPER)共同完成。在 Informix 中，数据库管理员(DBA)具有最高权限，他甚至可以删除任何数据库对象而不需考虑该对象的拥有者。在 Oracle 中，系统管理员具有对数据库的系统权，强大的系统权可在系统范围内执行各种操作。另外，还有数据库属主和数据库对象属主，数据库属主拥有对该数据库的各种权限。数据库对象属主具有对该对象的所有权限，可以对所拥有的对象执行各种操作。

(3)身份认证(Authentication)。是为了确定某人是它自称的那个人，并核查其合法性。在当前流行的这几种 RDBMS 中，身份认证一般有三级：系统登录，数据库连接和数据库对象使用。系统登录一般由操作系统提供检查，要求用户输入用户名或口令加以验证。一旦通过系统安全检查，当要求访问数据库时，就要与数据库进行连接，由数据库管理系统验证用户身份并作合法性检查。在对数据库中对象进行操作之前，数据库管理系统也要作身份验证，核实该用户是否具有权对该数据库对象进行指定的操作。当然，各种 RDBMS 的身份验证的具体做法也不尽相同，在本文稍后阐述。

(4)自主访问控制(Discretionary Access Control——DAC)。是根据用户的身份或角色来控制对数据库及数据库对象的访问，是对数据库访问的一种限制。这种类型的访问控制取决于具有某些权限的用户的意愿，能够直接或间接地将其所具有的权限转让给其他用户，基于这种意义的访问控制是自主的。

在当前流行的这几种 RDBMS 中，采用著名的存取矩阵模型来实现自主访问控制。存取矩阵模型是一张二维表，描述用户对数据库及其对象的访问权限(或称访问关系)，这是通过 GRANT 语句来建立的。可以根据实际应用需要加以扩充，例如，对访问时间的限制、访问历史记录的限制、可以同时读取信息项个数的限制等等。在实际使用时，由于存取矩阵大而稀疏，一般不宜直接采用，而采用按行存储法、按列存储法、锁钥法、口令密码法等几种实用技术来具体实现。

(5)审计(Auditing)。审计是通过跟踪并记录用户对数据库和/或数据库对象的创建、修改、删除，特定角色激活的用户的所有活动，权限的授予、收回，数据库数据的装入、卸出，用户注册或退出等。在当前流行的这几种 RDBMS 中，都提供了审计功能。一般审计的内容分为固定和选择两部分：固定的审计内容是确立审计功能后审计系统自动对其进行审计；选择的审计内容是由用户(包括 DBA)通过某种设置方式或命令方式来指定的。

4. 当前为安全机制所作的努力和改进

从上述对当前流行的数据库管理系统安全机制共性的剖析，可以认为它们大都符合美国国防部颁发的可信计算机系统评估标准(TCSEC)中的 C 类的 C1 级或 C2 级要求。但是，当前信息系统所基于的网络化的开放环境，提高了数据集成的优越性，却

降低了分离系统所固有的安全性。为了使产品能适应开发信息系统的网络化新环境，各厂家对自己的产品作了许多改进，使他们产品的版本不断提高，其中重要的改进是安全机制的改进，目标是实现多级安全机制，并努力达到 TCSEC 的 B 类（主要是 B1 级或 B2 级）标准。

Oracle 公司的 Trusted Oracle7 是一个多级安全数据库服务器，它不仅包括 Oracle 协同服务器的所有功能与特征，还特别增强了作为多级安全标志的两个特征：强制访问控制和使用标签。Trusted Oracle7 在任何一个用户访问数据库之前，首先对它进行强制访问控制。数据库中的每一行都有一个安全标签，用以表示该行数据的敏感度。每一用户可以写的数据的敏感度标签必须与他当前任务的敏感度标签相同（同级写），每一用户可以读的数据的敏感度标签必须等于或小于他当前任务的敏感度标签（下读）。这样的安全策略能够阻止用户将高敏感度的数据"向下写"到低敏感度对象中。同样，数据从高敏感度的对象读入低敏感度的对象或进程也是被禁止的。每个用户还被授予一定的权限，这种权限限制他不能连接到敏感度标签在其权限范围以外的系统，即他无权访问那些敏感度标签在他权限范围以外的系统中的数据。

Sybase 公司和 TRM 合作开发符合 TCSEC 的 B 类标准的 Sybase 安全 SQL 服务器（Sybase Secure SQL Server），它是网络数据库服务器。Sybase 安全 SQL 服务器有两个版本：B1 版在具有 B1 级安全的 UNIX 操作系统上运行；B2 版据称可在裸机上运行（无操作系统），它包含一个专用通信接口，用以与客户进程之间进行通信。Sybase 安全 SQL 服务器提供强制访问控制、自主访问控制、安全事件审计、以及系统安全员/系统管理员/数据库属主/一般用户工作范围的逻辑分工。它还提供 TCSEC 的 B2 级保障：要求可信计算基（TCB）与非可信软件分离，TCB 总是自行保护且具足够小的检验和测试。Sybase 安全 SQL 服务器提供完整性保障：数据库中的每一页都含有循环冗余检查，以保证事务的永久性；整个系统使用内部检查来保证数据库的完整性。Sybase 安全 SQL 服务器的性能损失小，可与非 B 类安全的 DBMS 相比拟。但是，Sybase 安全 SQL 服务器目前还未进入我国市场。

Informix 公司的联机/安全动态服务器（Informix-Online Dynamic Server）是一个对安全 UNIX 和 CMW 平台特许的部件，它支持强制访问控制（MAC）、系统范围离散特权、数据标签、以及审计跟踪机制。

IBM 公司的 DB2 主要对用户的身份验证上作了改进。用户对数据库的访问首先在 DB2 之外被认证。当一个数据库实例在服务器上被创建或被编目时，或在远程节点上被编目时，就为该数据库实例指定一个认证类型。认证类型决定当访问服务器上的数据库时对用户进行验证的位置和方式。认证类型分为：CLIENT，SERVER 和 DCS。如果认证类型是 CLIENT，说明用户的身份验证在激活应用的服务器上进行；如果认证类型是 SERVER，说明用户的身份验证将在数据库所驻留的服务器上进行，若已经安装了分布式数据库连接服务器（DDCS），则将在安装了 DDCS 的网关上对用户身份进行验证；如果认证类型是 DCS，验证将被传递到主机数据库管理系统。若数据访问未涉及 DDCS，则将在数据库驻留的服务器上对用户进行身份验证。

Microsoft SQL Server 在用户登录到 Windows NT 并与数据库建立了信任连接后，当需要与数据库连接时，就可利用信任连接而不必再次输入口令了。

结束语 本文对当前流行的几种数据库管理系统的安全机制进行了综合剖析，目的是使读者能对它们的安全机制有一定的了解，以便在开发信息系统时，能从中得到一些启发和参考，根据用户对新系统数据库安全性的实际需要和可能，合适选择数据库管理系统或它们的强化安全机制部件。

当然，这里的综合剖析只能是一种基于"快照"的剖析，各厂家的 RDBMS 将随着应用对数据库安全性需求的提高和时间的推延而加强。

参考文献

1 Research Direction in Database Security, Workshop. Menlo Park, California, May 1998. 24～26

2 Database Security, DBMS, February 1997 Server Side. Avalable at. http: // www. dbmsmag. com/9702d17. html

3 本文中提到的几种 RDBMS 的有关资料