安全数据库概述与前瞻

Secure DB and Its Developing Trends

李黎明 （上海警备区司令部自动化工作站 200040）
秦小麟 （南京航空航天大学信息科学与技术学院 210016）

摘要：安全数据库的基本概念包括可信计算基、主客体分离、身份鉴别、数据完整性、自主访问控制、审计、标记与强制访问控制、数据安全模型形式化和访问监控器等。对于访问控制策略、数据库安全模型、数据库入侵检测和数据库入侵限制及恢复技术是今后研究的重要方向。

关键词：安全数据库 可信计算基 TCSEC 入侵限制 入侵恢复

数据库技术产生于六十年代末，是信息系统的核心和基础，它的出现极大地促进了计算机应用向各行各业的渗透。随着数据库应用的广泛深入，数据库安全方面的需求越来越突出。安全数据库方面的研究得到了极大的关注。

1 安全数据库的基本概念

要理解安全数据库，我们首先要了解以下基本概念：

1.1 可信计算基

可信计算基是指为实现系统安全保护策略的各种安全保护机制的集合。它是数据安全的基本概念。

1.2 主体、客体与主客体分离

主体是数据的访问者，包括用户、应用程序、进程以及线程等。客体是数据及其载体，包括表、视图、数据文件、磁盘区域、内存区域、存储过程等。与数据安全有关的实体是独立的并且只能是主体或是客体，主体子集和客体子集是两个独立的互不相交的的子集。主、客体集间存在单向（主体向客体）访问关系。

1.3 身份鉴别

身份鉴别就是主体访问客体前，系统要求主体用一定标志标识自己身份。可信计算基使用这些标志以鉴别用户身份，并阻止非法主体的访问。身份鉴别方法有：口令、指纹等。

1.4 数据完整性

数据完整性指保护数据的修改并保持其一致性。通过完整性策略阻止非授权主体修改或破坏数据。在网络环境下可使用敏感标志以确保数据在传输中不被破坏。

1.5 自主访问控制

即可信计算基定义和控制系统中命名主体对客体的访问，实施机制（如访问控制表）允许主体规定和控制对客体的共享，并阻止非授权主体访问客体。自主访问控制适合在单机方式下的访问控制，并允许规定客体的共享控制。可以通过主体授权形式任意改变主体访问客体的权限。

1.6 审计

指设置审计功能记录可疑主体访问客体的轨迹，以防止非法主体对客体的访问。

记录的内容包括：访问时间、用户、操作类型、是否成功等。

1.7 标记与强制访问控制

它是与自主访问控制是完全不同的访问控制手段。需对主体与客体加上标记，标记可以是一个数字或一个字母集合。一般有两种标记：一是安全级别标记，是一个数字，规定了主客体的安全级别，只有主体级别高于客体级别时，才允许访问；另一个是安全范围标记，是一个字母集合，规定了主体的访问范围，只有主体的标记包含或相等于客体的标记时才允

许访问。

强制访问控制的操作如下：对每个主、客体打上两个标记，安全级别标记和安全范围标记。主体访问客体时由 TCB 检查标记，只有主、客体的两种标记都符合允许条件时，才允许主体访问客体。

1.8 数据安全模型的形式化

由于数据安全模型其内在安全关系的复杂性与多样性，需要建立一个有效的形式化体系，用以把握所提出的安全需求并填补安全漏洞。形式化系统可以实现对模型形式化验证与发现安全漏洞、隐蔽通道。

1.9 访问监控器

上述安全功能需要一个独立的抗篡改的复杂度足够小的系统实体（访问监控器），以实现数据安全。访问监控器在功能上仲裁主体对客体的全部访问。它是一个独立的物理机构，由一定的硬件与软件组成。

2 数据安全的级别

2.1 美国颁布的信息安全标准

1985 年，美国颁布《可信计算机系统安全评测标准》TCSEC（Trusted Computer System Evaluation Criteria），把数据安全级别划分为四类七级：

D 级：无安全保护的系统。

C1 级：具有主体、客体及主客体分离、身份鉴别、数据完整性、自主访问控制功能的系统；核心是自主访问控制。

C2 级：满足 C1 级全部功能，且具有审计功能的系统；核心是审计功能。目前国内使用的系统大部分符合此标准。

B1 级：满足 C2 级全部功能，且具有标记及强制访问控制功能的系统；核心是强制访问控制。国际上有部分系统符合此标准，国内基本上没有满足此标准的系统；满足此标准的系统可称为可信系统或安全系统。

B2 级：满足 B1 级全部功能，且具有形式化安全模型与隐蔽通道功能的系统；核心是形式化安全模型。目前国内外均无满足此标准的系统。

B3 级：满足 B2 级全部功能，且具有访问监控器功能的系统；核心是访问监控器。目前国内外均无满足此标准的系统。

A 级：更高的形式化要求。目前国内外均无满足此标准的系统。

2.2 我国的信息系统安全评估标准

1999 年我国颁布了信息安全评估级别，共分为五级与美国标准的对应关系如下：

第一级：用户自主保护级 C1 级

第二级：系统审计保护级 C2 级

第三级：安全标记保护级 B1 级

第四级：结构化保护级 B2 级

第五级：访问验证保护级 B3 级

2.3 目前常用系统的安全级别

目前市面上常用软件经过权威机构的评测，确定了其安全级别。如 Oracle、Sybase、Informix、SQL Server 等数据库系统软件符合 C1 或 C2 级安全要求；Windows、Unix 操作系统符合 C1 或 C2 级安全要求。市场上大部分系统软件都处于 C1 或 C2 级安全级别。此外，美国有符合 B1 级的军用版本 Oracle 数据库系统和 WinNT 操作系统。国内有一些符合 B1 级的安全原型 DBMS：如 OpenBASE、Cobase 等。

3 传统的数据库安全技术

传统的数据库安全技术主要研究：预防技术、身份认证、存取控制模型（自主存取控制、强制存取、基于角色的存取控制等）、合适的 DBMS 配置、管理、数据库设计、备份和检查点技术等内容，以及预防技术与操作系统级、网络级安全、防火墙等安全技术的集成等方面的内容。

其中心是以预防为中心的被动保护安全机制，它主要着眼于对外部用户的身份和权限约束的检查。这种安全机制无法做到防止所有的非法攻击，并且对于合法用户的权限滥用，它常常显得无能为力。此外以预防为主的安全机制也难以满足一些重要信息系统如交通、银行等关键系统的可生存性要求。因此安全数据库的研究开发就显得更为迫切。

4 安全数据库的研究方向

安全数据库的研究方向主要包括以下四个方面：

4.1 访问控制策略

自主访问控制（DAC）策略和强制访问控制

(MAC)策略是访问控制策略研究的两个主要方向。

4.2 安全模型

当前研究的安全模型包括存取矩阵模型、Take – Grant 模型、动作 – 实体(Action – Entity)模型、信息流控制格模型、Bell – La Padula 模型、基于角色的访问控制(RBAC)模型、Biba 模型、Dino 模型、安全数据视图模型、Smith &Winslett 模型等。

其中角色管理机制(RBAC)受到越来越广泛的关注。RBAC 模型将权限组织成角色,用户通过获得角色成员的资格来行使权限,这大大减化了权限管理的复杂性。更重要的是 RBAC 是政策中立的,RBAC 模型可以实施 DAC 和 MAC 两种存取控制。虽然这些模型是从信息安全角色提出的,但其原理仍适用于数据库领域,并有成功的运用。

多级安全数据模型,即实现一个多级关系的安全数据模型和基于角色和强制存取的混合存取控制模型,即实现一个基于角色的强制存取控制模型是今后研究的主要方向。其中基于角色的访问控制和基于属性标记的强制安全策略相结合的存取模型理论和实现是需要解决的关键技术问题。

4.3 数据库入侵检测

数据库入侵检测不同于网络的入侵检测,必须从多个层次上对用户的行为进行检测。有学者提出可以针对数据库模式之间的关系,通过模式的主键和外键的函数依赖来确定查询属性之间的关系参量来检测异常。还有学者提出可以对数据库事务活动的异常进行监控,或者通过捕获数据库的应用语义来检测数据库应用程序的异常。由于数据库结构的复杂性,数据库入侵检测技术面临着更多的研究难点,技术上还处在研究阶段。

结合操作系统与网络的入侵检测方法,研制数据库入侵检测的算法与理论;研究具有安全检测、防范功能的规则子系统是今后研究工作的重点。新的数据库入侵检测算法和理论的提出对数据库入侵检测起着重要指导作用。

4.4 数据库对入侵的限制和恢复技术

入侵限制方法有静态分区法、数据标记法、多阶段隔离法、多版本法等。有学者提出对数据库事务活动的异常进行监控,或者通过捕获数据库的应用语义来检测数据库应用程序的异常。

入侵恢复与传统数据库恢复的不同点在于入侵恢复往往需要在运行时恢复且可能需要撤消已提交的恶意事务。数据库恢复技术可分为两个阶段:第一阶段是确定应该撤消的事务。可以利用事务之间通过对数据读写形成的依赖关系或数据本身存在的依赖关系来确定。第二阶段是撤消已提交的事务。可以更新和利用传统恢复机制中的回滚或补偿等方法来实现。

今后主要研究方面在数据库入侵限制模型,即实现一个对入侵和怀疑用户进行隔离的模型和环境,并可以对隔离数据进行合并或抛弃机制;数据库入侵恢复模型,即实现具有撤消已提交恶意事务和运行时恢复数据库机制。数据库入侵限制模型和数据库入侵恢复模型是重点需要解决的关键技术问题。

我们相信对安全数据库的深入研究必将对数据库领域产生巨大的影响,极大丰富数据库的应用。

参考文献

1 Liu P. Architectures for Intrusion Tolerant Database Systems [C]. In: Proc. of 18th Annual Computer Security Applications Conf. Las Vegas, Nevada, Dec. 2002.

2 Ammann P, Jajodia S, McCollum C D, Blaustein B T. Surviving information warfare attacks on databases [C]. In: Proc. of the IEEE Symposium on Security and Privacy, Oakland, CA, May 1997. 164 ~ 174.

3 Yip R, Levitt K. Data Level Inference Detection in Database Systems[C]. In: Proc. of the 11th IEEE Computer Security Foundations Workshop, Rockport, Massachusetts, June 1998. 179 ~ 189.

4 Castano S, Fugini M G, Martella G, Samarati P, Database Security [M]. Addison – Wesley, 1995.

5 钟勇、秦小麟,数据库入侵检测研究综述[J],计算机科学,2004,31(10):15 ~ 18。

6 张剡、夏辉、柏文阳,数据库安全模型的研究[J],计算机科学,2004,31(10):101 ~ 103。