基于免疫体系的安全数据库结构设计研究*)

钟 勇 秦小麟
(佛山科学技术学院信息与教育技术中心 佛山 528000)
(南京航空航天大学信息科学与技术学院 南京 210016)

摘 要 提出了基于免疫体系的安全数据库四层结构:身份认证层,存取控制层,约束安全层,适应性检测层。并给出了约束安全层和适应性检测层的子层结构。将约束安全层分为完整性约束、分级和推理约束、访问约束和应用语义约束四个子层,将适应性检测层分为数据库活动级、关系模式级、事务级和应用语义级四个子层。构造了一个多层多级的数据库安全体系,最后给出了具体实现方案。

关键词 免疫系统,数据库安全,数据库滥用,滥用检测

Research on System Architecture of Secure Database Based on Immune Architecture

ZHONG Yong QIN Xiao-Lin
(Information and Education Technology Center, Foshan University, Foshan 528000)
(Information Science and Technology Institute, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)

Abstract This paper presents a secure database based on immune architecture. The architecture has four tiers including identification and authentication layer, access control layer, constraints security layer and adaptive detection layer. The paper also discusses the structures of the sub layers of the constraints security layer and the adaptive detection layer. The constraints security layer consists of integrity constraints, classification and inference constraints, access constraints, and application semantics constraints. The adaptive detection layer consists of active database level, relation schema level, transaction level and application semantics level. The paper outlines a multilayer and multilevel database security architecture. At the end of the paper, a detailed implementation is demonstrated.

Keywords Immune system, Database security, Database misuse, Misuse detection

1 引言

数据的保密性,完整性和可用性是数据库安全研究领域主要关心的问题[1],围绕着这三个目标,大量的研究从各个角度和关心的重点对一系列的问题进行了阐述。如各种授权机制[2]、授权模型(DAC[3],MAC[3],RBAC[4]),推理控制[5],多级安全数据库[6],多级安全事务[7],数据库误用检测[8],入侵容忍[9]、限制[10]和恢复[11]。既然数据库的安全需要是多方面的,多层次、单一的安全措施无法满足数据库安全的这些需要。因此,数据库的整体安全需要有一个统一的安全框架和理论基础。

人体作为长期进化的产物,具有很强的生存能力,其对病原体的免疫能力,抗伤害和维持身体正常运转的能力,坏死器官隔离和恢复能力(如再生等),异体器官排斥(如移植器官异体排斥),形成了一个精密完善且具有自我调节的智能安全系统。特别是人体的免疫系统(biological immune system IS)是一个高度复杂,并行,自适应以应付外来感染的信息处理系统。IS 系统的多层次多样性,分布性,错误容忍性,动态性,自我调控和适应性,使其具有今天的人工信息系统所最需要的一些特征如健壮性,适应性和自治性[12]。

在计算机安全特别是入侵检测领域对 IS 系统的模仿主要集中在操作系统和网络安全领域,操作系统模仿 IS 系统对本体(self)和异体(nonself)的识别机制,T 细胞的负选择生成机制(negative selection)通过系统调用序列来构造基于主机的入侵检测系统[13],网络入侵检测更重视对 IS 系统的分布性和自治能力的模仿[14]。在数据库安全领域,数据库的生存能力,自我修复能力,多层次的防护能力成为研究的重点。对 IS 系统防御体系和生存能力的模仿,可以把数据库设计成一个具有多层次防御能力,安全环境自适应,具有较强生存能力的安全系统,满足数据的保密性、完整性和可用性的要求。

2 人体免疫系统

免疫系统是人体生存能力中最重要的部分。如图 1 所示,它分为四层。第一层是皮肤层,是人体的第一道防线,第二层是生理层如人的体温,pH 度,生理层通过人体独特的生理条件形成不适合病原体的生长环境。第三层是先天性免疫层,先天性免疫层是预定的基于遗传的非自适应检测系统,类似于数据库中的约束条件或基于规则的检测系统。先天性免疫层能防止早期感染,提供人体对病原体的快速反应。先天性免疫层使用溶胞或吞噬等手段清除病原体。免疫系统的最后一道防线是获得性免疫层。获得性免疫层是免疫系统中能够自我学习的自适应机制,对新的病原体获得性免疫层产生初级反应消除该病原体并保持对该病原体的记忆。当第二次再遇到此种病原体产生更快更有效地次级反应清除病原体。

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

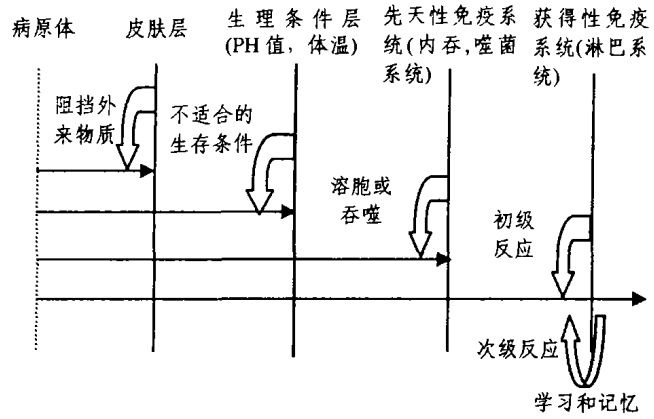

图 1　免疫系统结构

如图 2 所示，获得性免疫层是一个分工专门化的多层次检测系统。获得性免疫层主要包括 B 细胞和 T 细胞。B 细胞用来识别病原体，T 细胞用来识别本体和异体。B 细胞通过与病原体的亲合度来识别病原体，当 B 细胞与某病原体的亲合度超过一定阈值后被激活。B 细胞有可能被人本身的正常细胞即本体激活。为避免这种情况，B 细胞的激活还需要 T 细胞的确认。T 细胞能够识别本体和异体，因为 T 细胞在生长过程中经过负选择淘汰。即与正常细胞亲合度过大的 T 细胞被淘汰，剩下只能识别异体的 T 细胞成熟。B 细胞激活后产生抗体细胞杀死病原体和产生对病原体的记忆细胞。

3　数据库免疫系统结构

以身份认证和存取控制为重点的传统数据库安全机制越来越无法满足现代数据库的需要，身份认证和存取控制主要着眼于数据库的保密性以及某些商业完整性（如 RBAC 中对责权分离和组织体系结构的模拟[4]），对数据本身的完整性和可利用较少涉及，而对于数据库安全来说，数据的完整性和可利用性具有和保密性同等地位的重要性，特别是数据库在受到攻击之后的恢复和生存能力，如在信息战[15]（Information Warfare IW）的条件下，信息战的防卫要求采取任何手段防止攻击。但是在现有的条件下我们必须承认防止信息攻击的手段是不充分的，在某种程度上不可避免，总有攻击能够取得成功，因此对攻击的识别和受到攻击以后恢复手段是必要的[16]。

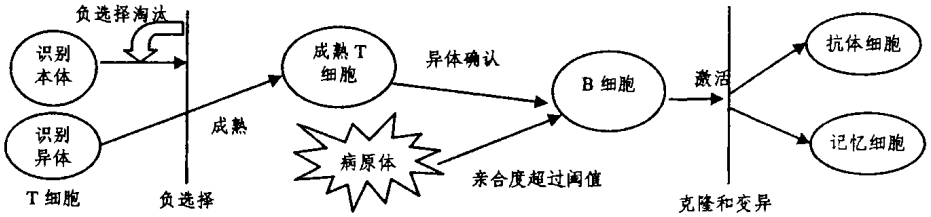

图 2　获得性免疫系统结构

计算机安全的主要威胁来自内部滥用而不是入侵[17]，这些内部滥用者往往具有合法的身份认证和授权。对于他们特别是系统管理员的滥用，传统的身份认证和授权机制有一定的限制。这使我们认识到，数据库必须具有多层次的防御体系，有自适应的自我检测能力。这正是免疫系统体系结构的优越所在。

人体免疫系统在体系结构上的特点是：①防御的多层次性。②防御功能的分工和专门化，不同的病原体由不同结构的 B 细胞来处理，而异我的识别则由 T 细胞来负责。③灵活和多样性的检测系统。先天性免疫系统可以看作是一个基于规则的检测系统，而适应性免疫系统是一个多层次的误用检测系统。这正适合于数据库活动的多层次性和多样性。本文的数据库免疫系统结构如图 3 所示。

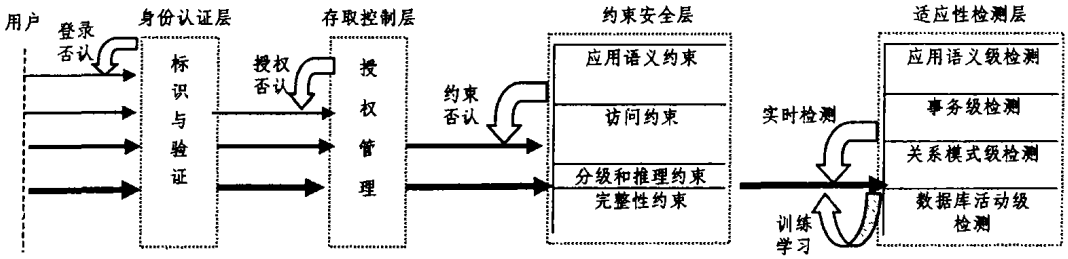

图 3　数据库免疫系统结构

身份认证是用户进入数据库的条件，存取控制层给出了用户活动的授权条件。

约束安全层是数据库的先天性免疫层，它由对数据库的约束条件组成，共分为四级。完整性约束由数据模式定义来实施，如多级安全模型 MLR[6]中的主键完整性，外键完整性，多实例完整性等。分级和推理约束是对安全数据库中的分级以及防止数据推理的限制条件。推理约束是用来防止使用低密级的数据推断出高密级的数据。分级和推理约束分为三类：基本分级约束，对数据库对象分级的约束，如某一元素、元组或字段的分级不能小于某一级；关联约束，对属性关系的约束，如病人和年龄之间的关系必须是保密级以上；推理约束，对推理属性的约束，如为了防止从病人的治疗医生及其专业推断出病人的病情，可以限制治疗医生及其专业的最小上界必须大于病人的分级。在文[5]中将分级和推理约束分为四类，其第四类相当于我们这里的完整性约束。访问约束是对用户或角色对数据访问的约束，如某些敏感数据只能在某一时间段才能被访问或修改，用户或角色在某一时间内访问过另一数据表则在一段时间内不能访问某一数据表，以及对查询返回数据基数的限制等。应用语义约束是根据数据本身的语义对数据所作的约束。例如用文[18]中的医生病人关系作例子，对医生病人数据语义的分析可以对数据的应用作出约束。比如医生只能查看他所治疗病人的资料和病历，医生开出的处方

只能是他专业范围内的，一个病人只能安排在一个病房内，病人的资料只能在一段时间后才可删除，某种病人不能吃某种食品，如果是儿童医院，病人的年龄不能大于某一年。应用语义约束是基于规则的异常检测系统。

免疫系统的适应免疫层是一个多层次专门化的滥用检测系统，数据库用户活动也是多层次的，为了检测的精确，多层次的滥用检测是必要的，低层次的验证可以帮助高层次的滥用检测[19]，在以往的研究中，或者是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[8,20]，或者是对数据库事务活动的异常进行监控[21,22]，或者捕获数据库的应用语义，如在文[18]中的医生和病人关系的例子中，病人服某种药的次数和剂量应与其它相同的处方之间有一定的相似处，病人购药的订单应大多数发生在白天上班时间等。不同的层次从不同的角度检测用户的活动，在这里我们将适应性检测层分为四级，对同一用户活动从不同的角度进行检测，使滥用检测更为精确，减少误警率。数据库活动级检测用户操作数据库的活动，如登录次数，试图违反授权或查询超出自己密级数据的情况。关系模式级检测用户会话中查询语句中的主键外键的函数依赖关系，因为在一个查询语句中同时出现的属性往往是它们之间存在着远近不同的函数依赖链，同时这些依赖链也可能影响它们在日志会话[8]中的支持率。事务级检测建立在用户查询的SQL语句和事务级的模式上。应用语义级检测建立在数据库数据的语义上，应用语义级是基于统计的异常检测系统。建立在这四个层次的上数据库滥用检测的具体实现模型限于篇幅，笔者将专文探讨。

4 NHSDB的具体设计

NHSDB(南航安全数据库)是我们正在开发的基于上述免疫机制上的安全数据库原型系统，NHSDB采取可信主体(Trusted Subject)[23]体系结构，由DBMS实施对主客体的标记和存取控制，基于多级关系数据模型MLR[6]，以角色存取机制作为权限管理的核心，采用角色管理政策的多策略模型实施可选的自主和强制存取控制，实施安全的两阶段锁协议[27]。

NHSDB基于NIST标准的角色存取机制RBAC[4]作为权限管理的核心。强制管理(MAC)作为角色的一种限制[24]来实现。对角色的管理可采取不同的配置以实施不同的安全策略。角色管理方式包括三种，自主式角色管理模块的配置可实现以属主为中心的传统自主存取DAC策略，类似于Oracle的角色管理机制。集中式角色管理的配置可实现集中式的角色管理，由主安全管理员(CSSO)统一管理角色用户的授权。层次式角色管理采用ARBAC99模型(URA99,PRA99)[25]的分层管理方式。存取控制层如图4所示。

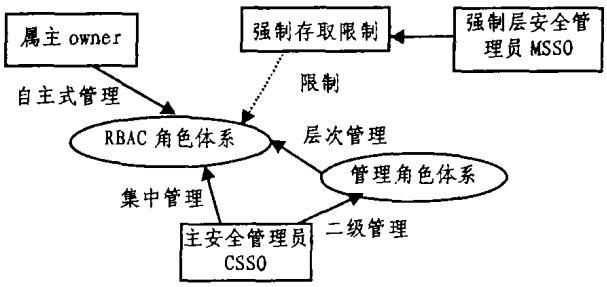

图4 NHSDB的存取控制结构

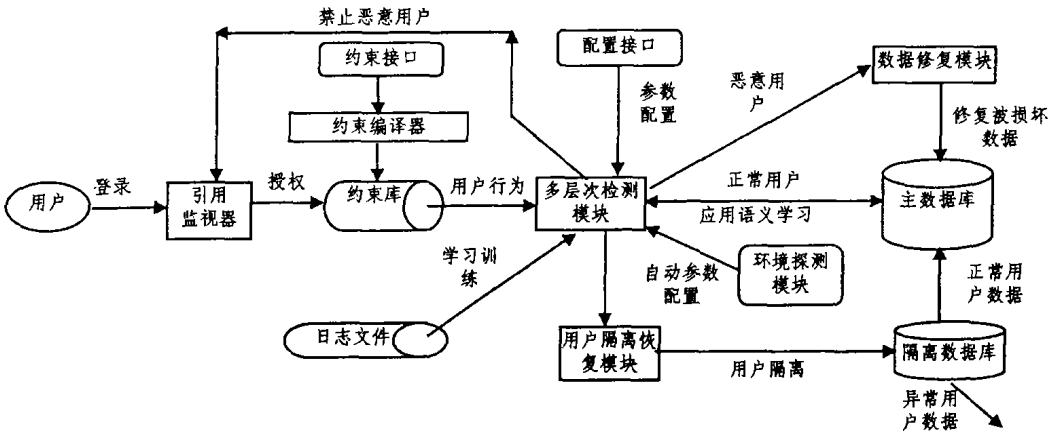

图5 NHSDB的体系结构

NHSDB免疫体系结构如图5所示，参考监视器[3]实施存取控制。多级关系数据模型MLR实现实体完整性(EI)，多实例完整性(PI)，数据借用完整性(DBI)，外键完整性(FKI)，参考完整性(RI)五种完整性约束。统一的外部约束接口，约束编译器对输入的约束进行编译。体系结构中增加了两个部件数据修复模块、用户隔离和恢复模块。在某种程度上总有攻击能够取得成功[18]，修复手段是必要的，数据修复模块用来去除恶意事务，恢复恶意用户所造成的数据毁坏，但要注意的是由于数据库中数据的扩散和传递性，数据的恢复可能造成良性事务的退出，具有不完全性[19]。另一方面，本体和异体的交集有时并不为空，对用户整体集U，正常用户集N，恶意用户集M，$U=N\cup M$，理论上$N\cap N=\phi$，实际中有诸多原因造成$N\cap N\neq\phi$，即检测的精度问题或其它原因存在不能确认的情况，比如用户S其行为略微偏离正常轨道，在不进一步观察的情况下无法确认是否为正常或恶意用户，如立即停止该用户的存取，如果后来证明该用户只是有不正常但合法的行为，停止存取将给该用户带来不必要的损失以及减少系统的可利用性，也不利于收集证据。但如果让该用户继续存取系统直到确认该用户的恶意行为，则可能给系统造成进一步的损失，这种用户是怀疑用户[26]，隔离和恢复模块用来将怀疑用户的数据与主数据库的数据隔离开来但允许该用户进一步操作，如用户最后证明是恶意用户，模块将用户数据与抛弃，否则将用户数据合并入主数据库，数据修复模块和隔离与恢复模块相当于人体的再生能力。

结论以及进一步的研究 多层多级免疫体系结构有效地提高了数据的安全性,特别是在信息战条件下的数据库生存能力,但该体系结构的复杂性也易影响数据库的性能,在原型开发中应注意:

1. 模块的可配置性。多级限制体系和多级检测体系的模块应是可选的,随安全性的需要可选择不同的体系层次。

2. 检测的复用性。操作系统和网络如果也有各自体系的入侵检测系统,数据库检测体系作为应用入侵检测是有可能复用它们的结果从而提高效率。

以下的一些内容是本文的进一步研究方向。

1. 数据库适应检测层的具体实现方法。

2. 高可信数据库(High Assurance)指那些满足可信任数据库评价准则 TCSEC B2 及以上级别要求的系统[3],高可信数据库要求可信模块足够小和简单,易理解,易验证。如何调整 NHSDB 的免疫体系构造达到这一要求的可信计算基(TCB)[3]。

3. 人体异体器官排斥功能表明人体可以识别自己的器官,数据库如何检测 DBMS 系统本身的可信模块和日志文件的可信度。

参 考 文 献

1 Castano S, Fugini M G, Martella G, Samarati P. Database Security. Addison-Wesley, 1995

2 Jajodia S, Samarati P, Subrahmanian V S, Bertino E. A unified framework for enforcing multiple access control policies. In: Proc. of ACM SIGMOD Intl. Conf. on Management of Data, Tucson, Arizona, United States, May 1997. 474～485

3 National Computer Security Center. Trusted Database Management System Interpretation of the TCSEC. NCSC-TG-021, Version 1, April 1991

4 Ferraiolo D, Sandhu R, Gavrila S, Kuhn D, Chandramouli R. Proposed NIST Standard for Role -Based Access Control. ACM TISSEC, August 2001, 4(3)

5 Dawson S, De Capitani di Vimercati S, Lincoln P, Samarati P. Maximizing Sharing of Protected Information. Journal of Computer and System Science, May 2002, 64(3): 496～541

6 Sandhu R, Chen F. The multilevel relational (mlr) data model. ACM Transactions on Information and System Security (TISSEC), 1998, 11(1): 93～132

7 Atluri V, Jajodia S, George B. Multilevel Secure Transaction Processing. Kluwer Academic Publishers, 1999

8 Chung C Y, Gertz M, Levitt K. DEMIDS: A Misuse Detection System for Database Systems. In: Third Annual IFIP TC-11 WG 11.5 Working Conf. on Integrity and Internal Control in Information Systems, Amsterdam, Netherlands, Kluwer Academic Publishers, 1999. 159～178

9 Luenam P, Liu P. The Design of an Adaptive Intrusion Tolerant Database System. In: Proc. of the IEEE Workshop on Intrusion Tolerant Systems. June 2002. 368～373

10 Liu P, Jajodia S. Multi-phase damage confinement in database systems for intrusion tolerance. In: Proc. 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, June 2001. 191～205

11 Ammann P, Jajodia S, Liu P. Recovery from Malicious Transaction. IEEE Trans. on Knowledge and Data Engineering, 2002, 14 (5): 1167～1185

12 Hofmeyr S, Forrest S. Architecture for an Artificial Immune System. Evolutionary Computation Journal, 2000, 8(4): 443～473

13 Forrest S, Perelson A S, Allen L, Cherukuri R. Self-nonself discrimination in a computer. In: Proc. of the 1994 IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA: IEEE Computer Society Press, 1994. 202～212

14 Hofmeyr S A. An Immunological Model of Distributed Detection and its Application to Network Security: [Ph. D. thesis]. University of New Mexico, May 1999

15 Graubart R, Schlipper L, McCollum C. Defending database management systems against information warfare attacks: [Technical report]. The MITRE Corporation, 1996

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

17 Carter, Katz. Computer crime: an emerging challenge for law enforcement. FBI Law Enforcement Bulletin, December 1996. 1～8

18 Sielken R S. Application intrusion detection: [Technical Report CS-99-17]. Department of Computer Science, University of Virginia, June 1999

19 Liu P. Architectures for Intrusion Tolerant Database Systems. In: Proc. of 18th Annual Computer Security Applications Conf. San Diego California, December 09-13, 2002

20 Chung C Y, Gertz M, Levitt K. Discovery of Multi-Level Security Policies. In: The Fourteenth Annual IFIP WG 11.3 Working Conf. on Database Security, Schoorl, The Netherlands, August 21-23, 2000. 173～184

21 Ingsriswang S, Liu P. AAID: An Application Aware Transaction-Level Database Intrusion Detection System: [Technical Report]. Dept. of Information Systems, UMBC, 2001

22 Lee S Y, Low W L, Wong P Y. Learning Fingerprints For A Database Intrusion Detection System. In: 7th European Symposium on Research in Computer Security (ESORICS 2002), Switzerland, October 2002. D Gollmann, G Karjoth, M Waidner. Lecture Notes in Computer Science, No 2502 Springer- Verlag, 2002. 264～280

23 National Computer Security Center, Auditing Issues in Secure Database Management Systems: [NCSC Technical Report-005]. Volume 4/5, May 1996

24 Sandhu R, Chen F. Constraints for role-based access control. In: Proc. of the first ACM Workshop on Role-based access control, Gaithersburg, Maryland, United States, November 30 - December 02, 1995, 14

25 Sandhu R, Munawer Q. The ARBAC99 Model for Administration of Roles. In: Proc. of the 15th Annual Computer Security Applications Conf. December 06-10, 1999. 229

26 Jajodia S, Liu P, McCollum C D. Application-Level Isolation to Cope With Malicious Database Users. In: 14th Annual Computer Security Applications Conf. Phoenix, Arizona. December 7-11, 1998. 73～82

27 Bertino E, Jajodia S, Mancini L V. Indrajit Ray: Advanced Transaction Processing in Multilevel Secure File Stores. IEEE Trans. on Knowledge and Data Engineering 1998, 10(1): 120～135