空间数据库管理系统 VISTA 的强制访问控制设计*)

施化吉[1] 李星毅[1,2] 邵学军[1] 鞠时光[1]

(江苏大学计算机科学与通信工程学院 镇江 212013)[1] (北京交通大学电子信息工程学院 北京 100044)[2]

摘 要 对象关系型数据库安全访问控制是数据库安全研究的焦点之一。本文以自主开发的空间数据库管理系统 VISTA 为例,从安全规则、安全属性、强制访问控制三个角度详细讨论了 VISTA 的 MAC 设计方法,定义了形式化的安全规则,给出了算法流程和相应的安全信息数据结构。该设计方案也适用于其他相似的对象关系型数据库系统。

关键词 空间数据库管理系统,强制访问控制,对象关系型数据库管理系统

Design of Mandatory Access Control in Spatial Database Management System VISTA

SHI Hua-Ji[1] LI Xing-Yi[1,2] SHAO Xue-Jun[1] JU Shi-Guang[1]

(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, Jiangsu 212013)[1]

(School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044)[2]

Abstract The security access control for object relational database is one of the challenges in database security domain. Taking the Spatial Database Management System (SDBMS)—VISTA, which is developed independently by ourselves, for an example, this paper particularly discusses the design of Mandatory Access Control (MAC) from safety rules, safety properties and MAC designing, defines the formalized safety rules, and presents the procedure of algorithm and corresponding data structure of the safe information. This scheme is also applicable to other similar object relational database management systems (ORDBMS).

Keywords Spatial database management system, Mandatory access control (MAC), Object relational database management systems (ORDBMS)

强制访问控制(Mandatory Access Control ,MAC)通过无法回避的存取限制来防止各种直接的或间接的攻击。系统给主体分配了不同的安全属性,并通过主客体的安全属性的匹配比较决定是否允许访问继续进行[1]。

当系统的安全策略命令如下时,出现了对强制访问控制的需要:(1)保护决策不是由客体的属主决定;(2)系统必须加强保护决策。强制访问控制主要的实现方法有 Bell-LaPadula (BLP)模型[2,3]、Biba 模型[4]、安全视图模型(SEA VIEW)[5]、Denning 提出的基于流控制的格模型[6]等。由于其他模型主要是基于 BLP 模型的改进,因此我们主要以 BLP 模型为研究对象,对 Bell-LaPadula 模型进行了适当修改;在原有 BP 模型的基础上针对安全度小粒度情况,定义了相关的安全规则,如面特性规则、隐蔽规则等,并在空间数据库管理系统 VISTA 中应用了该 MAC 安全策略。VISTA 系统是我们课题组自主开发的一个空间数据库管理系统[7,8],并于 1992 年在该系统的基础上为墨西哥石油公司开发了一个用于石油勘探资源管理的 GIS。该系统由两部分组成:图符化数据库查询语言 CQL 和空间数据库管理系统。CQL 用可视化的方法进行数据库查询操作,空间数据库管理系统部分主要实现对空间数据库的维护操作,可以独立构成一个 ORDBMS。由于 VISTA 系统涉及众多敏感数据,为此在安全访问控制方面提出了较高的要求。本文主要讨论 VISTA 中的 MAC 设计方法。

1 相关安全规则

1.1 符号描述和基本定义

为便于描述,我们首先约定一组符号描述和有关的概念定义。

约定 1(符号描述):

(1)用如下符号描述安全数据库中的名词:M 表示"主体",O 表示"客体",S 表示"密级",P 表示"权力"。

(2)用 RD 表示数据库中满足关系型数据结构的数据对象,OC 表示对象类,OD 表示满足对象型数据结构的数据对象。Table(a)表示数据表 a,Record(a)表示记录 a 或元组 a,Field(a)表示字段,Attribute(a)表示对象 a 的属性,Operate(a)表示对象 a 的服务。View 表示视图。

(3)用 OP(name, M, O)表示操作原语,其中:name 为原语名,name∈{write, read, create};M 为操作发起的主体,O 为操作对象,即操作施加的客体。

(4)用 dom(a)表示对象的定义域,其中 a 为对象。如 dom (PR)表示定义给角色 R 的特权域。dom(O)表示系统辖域中的所有客体,而 dom(OS) 则表示密级为 S 的对象构成的集合。

约定 2(规则的符号描述):

$f:\subseteq a_1\times a_2\times\cdots\times a_n\rightarrow a_n$ 表示名为 f 的规则,$a_i(i=1,2,\cdots,n)$为规则的约束条件,a_0 为规则的作用结果。在不产生歧义的情况下用(f)表示规则名。

1.2 相关安全规则描述

安全规则是系统实现安全目标的准则,使系统进行安全控制的依据。在 VISTA 中定义了一套完整的安全规则,本文仅罗列与 MAC 相关的规则如下。

*)本课题得到国家自然科学基金(60173064)和江苏省自然科学基金(BK200204)的资助。**施化吉** 副教授,博士研究生,主要研究方向:数据库及信息安全技术;**李星毅** 博士研究生,主要研究方向:数据库及信息安全技术、交通信息工程及控制技术;**邵学军** 副教授,主要研究方向:空间数据库技术;**鞠时光** 教授,博导,主要研究方向:信息系统安全、空间数据库技术。

定义 1(主体密级规则(S1)) 只有特权角色主体可以定义或操纵主体的密级。即

规则(s1). $M_1 \times \underline{R_1(M_1)} \times M_2 \rightarrow S(M_2)$

定义 2(客体初始化密级规则(S2)) 包含四条规则:①客体继承宿主主体的密级;②子类客体继承所有父类客体密级的最低密级;③对象实例客体继承对象类的密级;④密级协调规则,当由规则(S2-1)、(S2-2)或(S2-3)组合定义客体密级,所得密级不一致时,以最低密级作为客体密级。规则描述如下:

规则(s2-1). $\overline{INITIALIZE}(O) \times M_0 \rightarrow S(O) = S(M_0)$

规则(s2-2). $\overline{INITIALIZE}(OC_0) \times \bigcup OC_{i_{father(OC_0)}} \rightarrow S(OC_0) = \min_i(S(OC_{i_{father(OC_0)}}))$

规则(s2-3). $\overline{INITIALIZE}(OD) \times OC_{OD} \rightarrow S(OD) = S(OC_{OD})$

规则(s2-4). $\overset{3}{\underset{i=1}{\times}} S(OD)_{(S2-i)} \rightarrow S(OD) = \overset{3}{\underset{i=1}{\min}} S(OD)_{(S2-i)}$

定义 3(客体密级修改规则(S3)) 包含两条规则:①客体密级可以由宿主主体修改,且新密级高于原密级及其主体密级;②客体密级可以由特权角色主体修改。规则描述如下:

规则(s3-1). $S(O) \times M_0 \rightarrow S'(O)\, I(S'(O) \geqslant \max(S(O), S(M_0)))$

规则(s3-2). $M_1 \times R_1(M_1) \times S(O) \rightarrow S'(O)$

定义 4(面特性规则(S4)) 组合客体的密级不高于其组成客体的密级。即

规则(s4). $O \times (O = \bigcup_i O_{i_0}) \rightarrow S(O) \leqslant \min_i(S(O_{i_0}))$

规则(S4)是数据库密级定义的一个重要属性,如:记录的密级不高于构成该记录的所有字段值的密级;对象实例的密级不高于其属性和方法的密级。该规则也可称为密级敏感性规则,即集体的成员至少和集体一样敏感。

定义 5(写规则(Wr)) 主体 M 对客体 O 进行写操作,必须满足两个条件:①M 对 O 有写访问权;②M 的密级不高于 O 的密级,或称 M 的密级被 O 的密级所支配。该规则可以描述为

规则(Wr). $M \times O \times P_{\overline{WRITE}(M,O)} \times (S_M \leqslant S_O) \rightarrow OP(write, M, O)$

定义 6(读规则(Re)) 主体 M 对客体 O 进行读操作,必须满足两个条件:①M 对 O 有读访问权;②M 的密级不低于 O 的密级,或称 M 的密级支配 O 的密级。该规则可以描述为

规则(Re). $M \times O \times P_{\overline{READ}(M,O)} \times (S_M \geqslant S_O) \rightarrow OP(erad, M, O)$

定义 7(建规则(Cr)) 主体 M 对客体 O 进行建操作,只需满足主体 M 具有创建客体的权力。该规则可以描述为:

规则(Cr). $M \times P_{\overline{CREATE}} \rightarrow OP(create, M, O) \times P_{\overline{WRITE}(M,O)} \times P_{\overline{WRITE}(M,O)}$

其中,主体 M 是客体 O 的宿主,M 对 O 拥有读和写的权力,并且是这两个权力的宿主。同时,根据规则(S2-1),此时被创建客体的密级等于主体的密级,即 $S(O) = S(M)$。

定义 8(视图重组规则(V)) 视图元组密级规则(V1):构成视图的元组密级最大上界不超过访问视图的主体密级。即

规则(V1). $View(a) \times M \rightarrow \max_i(S(Record(b_i)_{View(a)})) \leqslant S(M)$

注意:根据(S4)这些元组中可能存在高于主体密级的字段值。

最大满足性规则(V2):在(V1)的前提下,满足主体访问请求的所有元组应当在视图中全部出现,即使存在多实例的情况。规则描述为:

规则(V2). $View(a) \times M \rightarrow \forall \mathrm{Re}\, cord(b)_{View(a)}$

部分隐蔽规则(V3):视图中出现高于主体密级的客体信息是隐蔽的,即视图的原子组成的密级被主体密级支配。即

规则(V3). $View(a) \times M \times O_{View(a)} \times (S(O)\, \mathrm{f}\, S(M)) \rightarrow \overline{HIDE}(O)$

全部隐蔽规则(V4):视图中的一个元组的所有字段值的最小密级高于主体密级,则该元组对主体不可见,即视图中不出现"NULL"元组。即

规则(V4). $View(a) \times M \times \mathrm{Re}\, cord(b)_a \times Field(c_i)_b \times (\min_i S(c_i)\, \mathrm{f}\, S(M)) \rightarrow \overline{HIDE}(b)$

2 系统安全级的定义

强制安全访问策略是基于系统元素密级(Classification)的。VISTA 模型的密级是如下四元素集合中的任一元素:{绝密(Top Secret)、机密(Secret)、秘密(Confidential)、公开(Unclassification)}。此集合是全序的,即

绝密 > 机密 > 秘密 > 公开

2.1 主体密级的定义、修改和存储

策略对系统中的每个用户分配一个安全级,称为允许安全级(Clearance),分配给用户的允许安全级反映对用户不将敏感信息泄漏给不持有相应允许安全级用户的置信度,用户能以受允许安全级支配任意安全级别向系统注册,用户激活的进程将被授予此注册安全级别。

VISTA 模型中,主体密级定义遵循安全规则(S1),根据规则主体密级只能由特权角色定义,其定义、修改过程如图 1 所示。

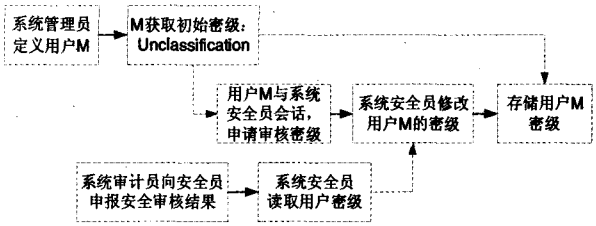

图 1 主体密级定义算法

当系统管理员定义一个新主体(用户)M 时,该用户获得初始化密级"公开"。主体 M 可以通过会话向系统安全员申请修改密级。此外,系统审计员根据安全审计结果,要求系统安全员对主体 M 的密级进行操作。只有系统安全员才能对主体密级进行修改。

VISTA 的主体密级存储在用户权限矩阵中,如图 2。

	S	O	属
M	S(M)	P	属
⋮	⋮	⋮	⋱

图 2 带主体密级的用户权限矩阵的逻辑存储结构

2.2 客体密级的定义、修改和存储

策略对系统中每个客户也分配一个安全级别,客体的安全级别反映了存储在客体内信息的敏感度,也反映了未经授权向

不允许存取该信息的用户泄漏这些信息造成的潜在损坏度。

在 VISTA 模型中，客体密级定义遵循安全规则（S2、S3 和 S4），其定义、修改过程如图 3 所示。

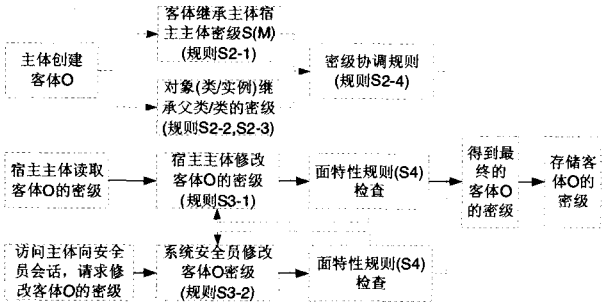

图 3　客体密级定义算法

根据图 3 可见，客体的定义和修改分三种情况：(1)创建主体，此时客体主要通过继承获得密级；(2)宿主主体修改所属客体的密级，此时遵循密级向上修改规则（规则 S3-1）；(3)特权修改，这种情况下只有系统安全员可以修改客体密级。

在 VISTA 系统中，用户定义的客体密级存储是我们关心的问题之一，用户定义的客体可以分为：库、表、索引、记录、对象类、对象实例、字段值、对象属性值等。图 4 给出了记录、对象实例、字段值、对象属性值和对象实例的方法等客体的密级存储结构。数据库、表、对象类的密级存储定义见图 5。

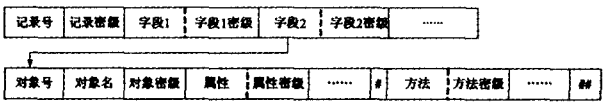

图 4　VISTA 数据逻辑存储结构

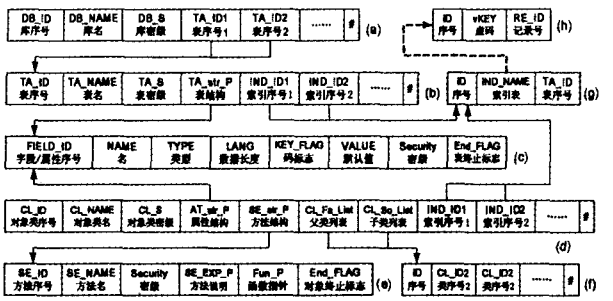

图 5　部分客体的逻辑存储结构

图 5(a)给出了库存储结构，DB_S 定义了库的密级，TA_IDi 给出了隶属于该数据库的表（“#”为终止符，下同）。

图 5(b)给出了表（含自由表）存储结构，TA_S 定义了表的密级，TA_Str_P 指向构成表的第一个字段存储结构的地址，IND_IDi 定义该表的索引序号。

图 5(c)给出了字段（对象属性）存储结构，字段为顺序存储，Security 定义了字段的密级，End_FLAG 定义了该字段（属性）是否为宿主表（宿主类）的最后一个字段（属性）。

图 5(d)给出了对象类的存储结构，CL_S 定义了类的密级，AT_Str_P 指向构成类的第一个属性存储结构的地址，SE_Str_P 指向构成类的第一个方法存储结构的地址，CL_Fa_List 为该类的父类列表，其值为“NULL”表示无父类，CL_So_List 为该类的子类列表，其值为“NULL”表示无子类，IND_IDi 定义该类表的索引序号。

图 5(e)给出了类的方法的存储结构，方法为顺序存储，Security 定义了字段的密级，End_FLAG 定义了该方法是否为宿主类的最后一个字段。

图 5(f)给出了类列表的存储结构，CL_IDi 为对象类序号。

图 5(g)给出了索引文件列表的存储结构。

图 5(h)给出了索引文件的逻辑结构。

图 4 和图 5 给出了 VISTA 模型中用户定义各种对象的存储结构，其中标志了强制访问控制所需的客体密级。

3　强制访问控制设计

强制访问控制通过判断主体密级与客体密级关系是否与操作规则匹配来控制操作是否合法。VISTA 中，规定了与强制访问控制相关的安全规则有写规则（Wr）、读规则（Re）和视图重组规则（V），前两者激活客体，后者反馈访问结果。强制访问控制算法如图 6 所示。

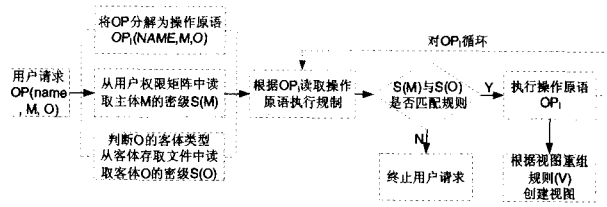

图 6　强制访问控制算法

强制访问控制首先将用户请求分解为操作原语请求序列，并读取相关客体和主体的密级；然后，依据操作原语请求序列逐个对操作原语请求的合法性进行甄别，若某个操作原语请求不合法，则终止用户请求；最后，若序列中所有原语请求均通过合法甄别，根据视图重组规则将请求结果反馈给用户。

结论　本文从安全规则、安全属性定义、强制访问控制三个角度讨论了 VISTA 中 MAC 的设计方法，实践验证具有良好的效果。VISTA 系统是一个空间数据库，设计关系数据为描述地理信息设计的对象型数据结构，故该设计方案亦适用于其他对象关系数据库。

由于在许多应用场所，对 MAC 中信息的完整性和保密性也很重要，但其控制方法同关系数据库的数据完整性控制，在此不再赘述。VISTA 系统中还涉及到授权问题，属于自主控制范畴，本文亦省略之。

参 考 文 献

1　Sandhu R S. Access Control: The Neglected Frontier. ACISP, 1996. 219～227

2　Bell D, LaPadula L. Secure Computer Systems: Mathematical Foundation and Model. Bedford, Massachusetts: Mitre Corporation, 1974

3　Bell D, LaPadula L. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Massachusetts: Mitre Corporation, 1976

4　Biba K J. Integrity consideration for secure computer system. Bedford, Massachusetts: Mitre Corporation, 1977

5　刘启原，刘怡. 数据库与信息系统的安全. 北京：科学出版社，2000. 322

6　Denning D E. A lattice model of secure information flow. Communications of the ACM, 1976, 19(5): 236～243

7　Ju Shi-Guang, Chapa S V, Chen wei-He. Extensible motor of a object-relational DBMS: design and implementation. In: The Proc. of Technology of Object-oriented Languages and Systems, IEEE Computer Society, 1999. 372～379

8　鞠时光. 可视化空间数据库查询语言 CQL. 计算机学报，1999，22(2)：205～211