基于可信验证的 DBMS 访问控制模型

牟亚莉[1,2],曾 浩[3]
MU Ya-li[1,2],ZENG Hao[3]

1.海军工程大学,武汉 430033
2.海军后勤部 信息化办公室,北京 100841
3.海军装备研究院,北京 100073
1.Navy University of Engineering,Wuhan 430033,China
2.Informationization Office of Navy Logistics Department,Beijing 100841,China
3.Navy Academy of Armament,Beijing 100073,China
E-mail:myl0521@sina.com

MU Ya-li,ZENG Hao.Credible validation based DBMS access control model.Computer Engineering and Applications, 2008,44(4):179-181.

Abstract: Actual access control model can't realize the system's security effectively.It presents an access control model for DBMS based on credible validation in trusted operation environment.The model can satisfy the system's requirements of security and integrality,realize the bidirectional flow of information at most,and also support the least privilege security characteristic.It is a flexible access control model on privilege distributing.

Key words: DBMS;trusted operation environment;access control;trusted validation

摘 要:针对目前访问控制模型在系统的安全实现方面存在的不足,在 RABC 的基础上,提出了可信操作环境下基于可信验证的 DBMS 访问控制模型,该模型满足系统的保密性和完整性需求,最大程度实现信息双向流动,同时支持最小特权安全特性,是一个权限分配灵活的访问控制模型。

关键词:安全数据库管理系统;可信操作环境;访问控制;可信验证
文章编号:1002-8331(2008)04-0179-03 **文献标识码**:A **中图分类号**:TP311

1 引言

随着可信计算理论与研究的发展,对于信息安全的防护已经逐渐从传统的被动防护转变为积极主动的防御[1],单一的安全策略模型已无法满足多样化的安全需求,而要想设计一个可有效地用于支持可信操作环境条件下的安全模型,必须站在可信计算平台[2]的角度。目前多数访问控制模型在数据库系统的安全实现方面都存在不足[3,4],其权限管理违反最小特权原则是导致 DBMS 安全漏洞的关键因素之一[5]。单纯的使用 BLP[6]模型和 BIBA[7]模型都无法解决数据库系统的安全性与完整性的协调问题,也无法实现信息的从高到低以及从低到高的双向流动。在设计数据库系统安全模型时主要考虑:解决数据库系统的安全性与完整性的协调问题,最大程度地实现双向信息流动;在实际数据库系统中,用户所扮演角色的级别、保密级别和完整性级别是统一的,高级角色较低级角色而言通常具有更高的保密身份级和完整身份级;系统模型支持最小特权安全特性,能够有效地实施用户权限的管理与扩展,实现权限分配灵活的访问控制模型。

当前的主流 DBMS 都支持基于角色的访问控制模型 RABC 的一些关键特性[8],此模型也是在 RABC 模型基础上,通过引入保密性与完整性可信验证机制提出了基于可信验证的访问控制模型 CVBACM(Credible Validation Based Access Control Model)。

2 可信环境下数据库系统安全公理

定义 1 可信操作环境 是基于可信计算平台(TCB),它能够为本地用户或者远程实体提供认证和授权服务,本地用户或者远程实体按照一组可预料的符合规定的行为模式进行操作并达到预期目的,则称这种操作环境是可信的。可信操作环境包括可信应用操作平台、应用区域边界安全以及网络通信安全。

由定义 1 推导出了信息系统安全公理 1,这是不需要证明的安全公理,也是信息系统安全所追求的目标。

信息系统安全公理 1 如果信息系统中每个用户都是经过认证和授权的,其操作都是符合安全要求的,那么就不会产生人为的攻击行为,就能保证整个信息系统的安全。

基金项目:国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z440)。
作者简介:牟亚莉(1976-),女,博士研究生,主要研究方向为:信息系统安全,数据库系统安全;曾浩(1976-),男,硕士,主要研究方向:计算机应用,信息系统工程。
收稿日期:2007-05-28 **修回日期**:2007-07-30

本地操作环境的可信建立在各个实体层的可信基础之上，包括可信硬件层、安全 OS 层、安全 DBMS 层、安全中间件层以及安全应用层。数据库系统作为本地环境的应用，其安全性与其他实体层关系密切，以下为可信环境下数据库系统安全公理。

数据库系统安全公理 1 如果数据库系统与其他层次的实体之间不存在实际的信息交换，那么该数据库系统是安全的。

数据库系统安全公理 2 如果数据库系统与其他层次的实体之间存在实际的信息交换，且访问请求的主体通过了数据库系统及其低层实体的可信验证，那么该主体对于数据库系统而言是安全可信的，主体的操作也是数据库系统及其低层实体许可的授权操作。

3 CVBACM 模型

3.1 基础元素

$USERS$,$ROLES$,$OBJS$,OPS,$PRMS\subseteq 2^{(OPS\times OBJS)}$分别表示用户集、角色集、对象集、操作集、权限集。在对象集中 $OBJ=\{obj_1, obj_2,\cdots,obj_t\}$为系统中固有的客体集合，$OBJ'=\{obj_1', obj_2',\cdots, obj_r'\}$为通过添加、创建等操作加入到系统中新的客体集合。TRANS 表示事务集，模型是针对 DBMS，因而采用事务代替 RABC 中的会话。

(1)$UA\subseteq USERS\times ROLES$，是用户到角色的多对多的映射关系。

(2)$PA\subseteq PERMISSIONS\times ROLES$，是授权到角色的多对多的映射关系。

(3)$Level(r)$：角色 r 在角色层次结构中所处的层次，用角色 r 的层次标示其保密身份级别和完整身份级别，即 $sl(r)=level(r)$,$w(r)=level(r)$。角色 r 在角色层次结构中所处的层次越高，其保密和完整身份级别越高。

(4)$Time(trans,r)$：角色执行事务的有效时间，如果它满足事务的时间要求，就以 $Time(trans,r)\leftrightarrow effective\text{-}time$ 表示。

(5)客体保密性许可范围集合 L，是客体保密性许可范围的量化标准，且保密性许可范围是符合系统安全策略要求的，$L=\{L_{obj}|obj_i\in OBJ\}$,$L_{obj}$ 表示客体 obj 的保密性许可范围。

(6)客体保密性可信验证函数 f_c f_c:$OBJS\rightarrow C$。保密性验证函数是客体 obj 到其保密性度量值 C 的映射。

(7)客体完整性许可范围集合 I，是客体完整性许可范围的量化标准，且完整性许可范围是符合系统安全策略要求的，$I=\{I_{obj}|obj_i\in OBJ\}$,$I_{obj}$ 表示客体 obj 的完整性许可范围。

(8)客体完整性可信验证函数 f_w f_w:$OBJS\rightarrow W$。完整性验证函数是客体 obj 到其完整性度量值 W 的映射。

3.2 系统状态

系统状态 V:v 是集合 V 中的元素，$v\in\{(op,f,p)|op\in OPS, f\in F, p\in PRMS\}$。$F=\{level(r), f_c, f_w\}$为访问级别函数集合。$op(r,obj,x,effect\text{-}time)$为一四元组函数，表示角色 r 在有效时间内执行事务而对客体 obj 的所实施的访问操作 x，$op\in OPS$，$x\in A$。访问模式集 $A=\{create, select, append, modify, delete\}$为系统中访问属性的集合，简化为 $A=\{\underline{c},\underline{s},\underline{a},\underline{m},\underline{d}\}$。

系统状态的转换由一组操作规则定义。规则 ρ 定义为：ρ:$R\times V\rightarrow D\times V$，其中，$R$ 为请求集；D 为请求的输出集，$R\times V$ 是在系统中为所有请求定义的请求-状态对集合；$D\times V$ 是在系统中为所有请求定义的决策-状态对集合。

关系 W 是状态转换集合，设 N 是状态序号集合，$N=\{1,2,\cdots i,\cdots\}$。定义系统 $\Sigma(R,D,W,z_0):=\{(x,y,z)\}$,$z_0$ 是系统的初始状态。其中 x 为 N 到 R 的函数，y 为 N 到 D 的函数，z 为 N 到 V 的函数，并且 $\forall t\in N$，当且仅当 $(xt,yt,zt,zt-1)\in W$ 时，有 $(x,y,z)\in\Sigma(R,D,W,z_0)$是系统 $\Sigma(R,D,W,z_0)$的呈现。

3.3 安全公理

安全公理 1 系统状态 $v=(op,f,p)$ 满足安全公理 1，iff，对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，下面的式子成立：

(1)$x=\underline{s}\Rightarrow sl(r)\geqslant sl(obj)\wedge w(r)\leqslant w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$；

(2)$x=\underline{a}\Rightarrow sl(r)\leqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$；

(3)$x=\underline{m}\Rightarrow sl(r)=sl(obj)\wedge w(r)=w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$。

可信验证安全公理 1 系统状态 $v=(op,f,p)$满足验证安全公理 1，iff，对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，下面的式子成立：

(1)$x=\underline{s}\Rightarrow sl(r)\geqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge f_w(obj)\in I\wedge Time(trans,r)\leftrightarrow effective\text{-}time$；

(2)$x=\underline{a}\Rightarrow sl(r)\geqslant sl(obj)\wedge f_c(obj')\in L\wedge Time(trans,r)\leftrightarrow effective\text{-}time$；

(3)$x=\underline{a}\Rightarrow w(r)\leqslant w(obj)\wedge f_w(obj')\in I\wedge Time(trans,r)\leftrightarrow effective\text{-}time$。

可信验证安全公理通过客体的保密性验证与完整性验证机制，保证系统的保密性与完整性。通过验证规则，使得高级角色在向低级角色下发信息时，通过保密性可信验证对信息进行检查，从而明确该信息的下发是否超出了保密安全策略要求所规定的范围，进而为该操作实施判断提供必要的依据，以保证系统的保密性。当低级别角色向高级别角色上报信息时，往往低级别角色所产生的数据含有病毒、逻辑炸弹和木马程序等的可能性很大，这些无疑对系统构成了较大的安全威胁，事实上，用于衡量完整性等级的术语是“可信度”，越高等级的数据具备越高的精确性和可靠性，因而需要对上报的信息进行完整性可信验证，从而明确该信息的上报是否超出了完整性安全策略要求所规定的范围，进而判断是否允许低级别角色上报该信息，以保证系统的完整性和可靠性。

3.4 操作规则

规则 1 对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，若 $x=\underline{s}$，iff，下面的一条成立：

(1)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj))\wedge w(r)\leqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time$；

(2)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time)\wedge f_w(obj)\in I$。

规则 2 对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，若 $x=\underline{a}$，iff，下面的一条成立：

(1)$obj\in trans(obj))\wedge sl(r)\leqslant sl(obj))\wedge w(r)\geqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time$；

(2)$obj\in trans(obj)\wedge sl(r)\leqslant sl(obj)\wedge w(r)\leqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time)\wedge f_w(obj')\in I$；

(3)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time)\wedge f_c(obj')\in L$；

(4)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj)\wedge w(r)\leqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time)\wedge f_c(obj')\in L\wedge f_w(obj')\in I$。

规则 3 对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，若 $x=\underline{c}$，iff，$obj'\notin trans(obj)level(r)\geqslant sl(obj')\wedge level(r)\geqslant w(obj')\wedge time(trans,r)\leftrightarrow effective\text{-}time$。

规则 4 对任意 $op(r,obj,x,effect\text{-}time)\in OPS$，若 $x=\underline{m}$，iff，下面的一条成立：

(1)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time)\wedge f_c(obj')\in L\wedge f_w(obj)\in I$;

(2)$obj\in trans(obj)\wedge sl(r)\geqslant sl(obj)\wedge w(r)\leqslant w(obj)\wedge time(trans,r)\leftrightarrow effective\text{-}time\wedge f_c(obj')\in L\wedge f_w(obj')\in I$。

规则 5 对任意 $op(r,obj,x,effect\text{-}time)\in OPS$,若 $x=\underline{d}$,iff,$obj\in trans(obj)\wedge level(r)\geqslant sl(obj')\wedge level(r)\geqslant w(obj')\wedge time(trans,r)\leftrightarrow effective\text{-}time$。

由数据库系统安全公理 1 可知,角色 r 执行创建或删除客体的操作,不存在与数据库系统以外的实际信息交换,因而不会影响数据库系统的安全性,但是删除客体的操作可能会破坏系统的完整性和可用性,经过数据库系统认证的可信用户,其操作也必须是数据库系统许可的授权操作,此处删除者的角色 r 所处的层次至少与被删除客体 obj 的保密级和完整级的相当,创建者的角色 r 所处的层次至少要与新创建的客体 obj' 的保密级和完整级的相当。

3.5 系统安全定理

定义 2 如果系统满足安全公理 1 和可信验证安全公理 1,那么系统是安全的。

定理 1 对于任何安全状态 z_0,$\sum(R,D,W,z_0)$满足可信验证安全公理 1,iff 对于每个行为$(r,d,(op,f,p),(op',f',p'))$,$W$ 满足以下条件:

(1)每个 $op(r,obj,x,effect\text{-}time)\in op\text{-}op'$满足可信验证安全公理 1;

(2)每个不满足可信验证安全公理 1 的 $op(r,obj,x,effect\text{-}time)\in op'$都不在 op 中。

证明 设$(x,y,z)\in\sum(R,D,W,z_0)$,且对于 $t\in N$,$z_t=(op_t,f_t,p_t)$。

(⇒)记 $op=op_t$,$op'=op_{t-1}$,假设$\sum(R,D,W,z_0)$对某个安全状态 z_0 满足可信验证安全公理 1,且 $op\ (r,obj,x,effect\text{-}time)\in op\text{-}op'=op_t\text{-}op_{t-1}$ 不满足可信验证安全公理 1,或不满足可信验证安全公理 1 的 $op(r,obj,x,effect\text{-}time)\in op'=op_{t-1}\subseteq op=op_t$;

$\because op_t\text{-}op_{t-1}\subseteq op$,且存在 $op(r,obj,x,effect\text{-}time)\in op_t$ 不满足可信验证安全公理 1,或存在属于 op_t 的 $op(r,obj,x,effect\text{-}time)\subseteq op_{t-1}$ 不满足可信验证安全公理 1;

$\therefore$ 存在安全状态 z_0,使得$\sum(R,D,W,z_0)$不满足可信验证安全公理 1,与假设相矛盾;

(<=) 归纳基础:$z_o=(op_o,f_o,p_o)$是安全的。

归纳假设:对 $t<n$,$z_{t-1}=(op_{t-1},f_{t-1},p_{t-1})$是安全的。设$(x_t,y_t,z_t,z_{t-1})\in W$,由(1)可知每个 $op(r,obj,x,effect\text{-}time)\in op_t\text{-}op_{t-1}$ 满足可信验证安全公理 1。

设 $op'_{t-1}=\{op(r,obj,x,effect\text{-}time)\mid op(r,obj,x,effect\text{-}time)\in op_{t-1}\wedge op(r,obj,x,effect\text{-}time)$不满足可信验证安全公理 1$\}$,根据(2)$op'_{t-1}\cap op_t=\phi$:

$\therefore op'_{t-1}\cap(op_{t-1}\cap op_t)=(op'_{t-1}\cap op_t)\cap op_{t-1}=\phi$,即如果 $op(r,obj,x,effect\text{-}time)\in op_{t-1}\cap op_t$,那么 $op(r,obj,x,effect\text{-}time)$不属于 op'_{t-1},从而 $op(r,obj,x,effect\text{-}time)$满足可信验证安全公理 1;

$\therefore$ 如果 $op\ (r,obj,x,effect\text{-}time)\in op_t$,那么 $op(r,obj,x,effect\text{-}time)\in op_{t-1}\cap op_t$,归纳假设保证 $op(r,obj,x,effect\text{-}time)$满足可信验证安全公理 1;

或者 $op(r,obj,x,effect\text{-}time)\in op_t\text{-}op_{t-1}$,(1)保证 $op(r,obj,x,effect\text{-}time)$满足可信验证安全公理 1:

$\therefore z_t=(op_t,f_t,p_t)$是安全的。

证明完毕。

定理 2 对于任何安全状态 z_n,$\sum(R,D,W,z_n)$满足安全公理 1,iff 对于每个行为 $(r,d,(op,f,p),(op',f',p'))$,$W$ 满足以下条件:

(1)每个 $op(r,obj,x,effect\text{-}time)\in op\text{-}op'$满足安全公理 1;

(2)每个不满足安全公理 1 的 $op(r,obj,x,effect\text{-}time)\in op'$都不在 op 中。

证明 同定理 1 的证明。

3.6 系统转换规则

定义 3 如果对于所有的$(r,v)\in R\times V$,v 满足安全公理 1,那么规则 ρ 是满足安全公理 1 的,其中 $\rho(r,v)=(d,v')$表示 v' 满足安全公理 1。

定义 4 如果对于所有$(r,v)\in R\times V$,v 满足验证安全公理 1,那么规则 ρ 是满足可信验证安全公理 I 的,其中 $\rho(r,v)=(d,v')$表示 v'满足可信验证安全公理 1。

定义 5 设 $\omega=\{\rho_1,\cdots,\rho_m\}$是规则集合。对于请求 $r\in R$,决策 $d\in D$ 和状态 $v,v'\in V$ 有$(r,d,v,v')\in W(\omega)$ iff $d\neq i$ 且存在唯一的整数 i,$1\leqslant i\leqslant m$ 满足 $\rho_i(r,v')=(d,v)$。

定理 3 设 ω 是满足安全公理 1 的规则集合,z_0 是满足安全公理 1 的状态。那么$\sum(R,D,W(\omega),z_0)$满足安全公理 1。

证明 假设$(x,y,z)\in\sum(R,D,W(\omega),z_n)$是不满足安全公理 1 的状态。

选择 $t\in N$,使得(x_t,y_t,z_t)为$\sum(R,D,W(\omega),z_n)$的第一个不满足安全公理 1 的状态。

$\because(x_t,y_t,z_t,z_{t-1})\in\sum W(\omega)$,由定义 4 存在唯一的规则 $\rho\in\omega$,使得 $\rho(x_t,z_{t-1})=(y_t,z_t)$。

由定义 3,规则 ρ 是满足安全公理 1 的,且 z_{t-1} 满足安全公理 1,那么 z_t 必须满足安全公理 1,与假设相矛盾,故假设不成立。

定理 4 设 ω 是满足可信验证安全公理 1 的规则集合,z_0 是满足可信验证安全公理 1 的状态。那么$\sum(R,D,W(\omega),z_0)$满足可信验证安全公理 1。

证明 同定理 3 的证明。

定理 5 设 $v=(op,f,p)$满足安全公理 1,$op(r,obj,x,effect\text{-}time)\notin op$,$op'=op\cup\{op(r,obj,x,effect\text{-}time)\}$,且 $v'=(op',f,p)$,那么 v'满足安全公理 1,iff 下面的条件之一成立:

(1)$x=\underline{s}\Rightarrow sl(r)\geqslant sl(obj)\wedge w(r)\leqslant w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$;

(2)$x=\underline{a}\Rightarrow sl(r)\leqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$;

(3)$x=\underline{m}\Rightarrow sl(r)=sl(obj)\wedge w(r)=w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time$。

证明 如果 v'满足安全公理 1,结论显然成立。

反之,如果(1)、(2)、(3)条件均成立,设 $op'(r,obj,x,effect\text{-}time)\notin op'$,$op'(r,obj,x,effect\text{-}time)\notin op$,假设 v 满足安全公理 1,那么 v'也同样满足安全公理 1,否则,$op'(r,obj,x,effect\text{-}time)=op(r,obj,x,effect\text{-}time)$,根据(1)、(2)、(3)条件和安全公理 1,$v'$满足安全公理 1。

定理 6 设 $v=(op,f,p)$满足可信验证安全公理 1,$op(r,obj,x,effect\text{-}time)\notin op$,$op'=op\cup\{op(r,obj,x,effect\text{-}time)\}$,且 $v'=(op',f,p)$,那么 v'满足验证安全公理 1,iff 下面的条件之一成立:

(1)$x=\underline{s}\Rightarrow sl(r)\geqslant sl(obj)\wedge w(r)\geqslant w(obj)\wedge Time(trans,r)\leftrightarrow effective\text{-}time\wedge f_w(obj)\in I$;

(2)$x=\underline{a}\Rightarrow sl(r)\geqslant sl(obj)\wedge f_c(obj')\in L\wedge Time(trans,r)\leftrightarrow effective\text{-}time$;

(3)$x=\underline{a}\Rightarrow w(r)\leqslant w(obj)\wedge f_w(obj')\in I\wedge Time(trans,r)\leftrightarrow$

(下转 218 页)