改进的操作系统安全访问控制模型

权义宁[1,2]，胡予濮[1]

(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071；
2. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘要：提出了一个基于多级安全策略的强制访问控制模型，它的保密性安全规则是基于 BLP 模型，而完整性安全规则是基于 Biba 模型. 由于 BLP 模型和 Biba 模型的信息流走向完全相反，简单将它们结合会引起对某些客体进行合法的访问遭到拒绝，因此对主体和客体引入了可信度策略，使得主体在进行合法的资源访问时不会因为安全级别较低而遭到拒绝，从而使保密性和完整性两个安全特性能够紧密地结合在一起. 该模型既能防止越权泄露信息，又能控制信息的非授权修改，从而同时保证了系统的保密性和完整性

关键词：多级安全策略；强制访问控制；安全模型；操作系统
中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2006)04-0539-04

An improved secure access control model in Operating System

QUAN Yi-ning[1,2], *HU Yu-pu*[1]

(1. Ministry of Edu. Key Lab. of Computer Networks & Information Security, Xidian Univ., Xi′an 710071, China; 2. School of Computer Science, Xidian Univ., Xi′an 710071, China)

Abstract: A mandatory secure access control model named SOSACM of Operating System that is based on the multi-level security policy is put forward. Its confidetiality inherits the BLP model, and its definition of integrity is on the basis of Biba model. But in fact, the simple conjunct of BLP and Biba models will make some legal object not accessible because the directions of information flow in the BLP model and integrity in the Biba model are opposite. In the model, a trusted level strategy that makes the combination of confidentiality and integrity property tight has been developed, which should ensure that subjects can access objects legally. The model will be beneficial to its application to constructing secure Operating Systems in future.

Key Words: multi－level security strategy; mandatory access control; security model; operating system

BLP 模型[1]是安全操作系统中最经典的多级安全(MLS)策略模型，但它只注重于系统安全的保密性方面，却没有考虑系统的完整性. Biba 模型[2]是另一个经典的多级安全策略模型，为了实现信息完整性的安全指标，它模仿 BLP 模型的信息保密级别，定义了信息完整性级别. Biba 模型通过“不向上写”使得高完整性级别信息的内容是由高完整性进程产生，从而保证了高完整性级别信息不会被低完整性的信息或者进程中的内容覆盖. 但是 Biba 模型却忽略了系统的保密性.

文[3]设计了一个军用安全操作系统(ASOS)，在该系统中，一个安全级定义了两个访问标记：一个完整性标记 ω 和一个保密性标记 λ，对 λ 应用 BLP 模型的强制访问控制规则，对 ω 应用限制的 Biba 模型强制访问控制规则. 这种方法虽然在一定程度上为系统提供了完整性策略，但它只是实现了简单的完整性规则. 这种简单组合存在的问题是：很可能造成合法的资源访问要求遭到拒绝. 为了解决这个问题，文献[4]提出了一种基于多级安全策略的二维标识模型. 这个模型是在对可信主体必须遵守最小特权原则的前提下，利用保密性

收稿日期：2005-08-19
基金项目：国家自然科学基金资助项目(60273084)
作者简介：权义宁(1969-)，男，副教授，西安电子科技大学博士研究生.

标识和可信度标识共同构成客体的访问表示,并定义了两个约束条件,从而既能防止越权泄漏信息,又能控制信息的非授权修改. 但是,该模型是在抛弃 Biba 模型的基础上,采用 BLP 模型并定义特权和可信度来代替 Biba 模型处理完整性约束条件的,并没有严格按照 Biba 模型来检查完整性.

笔者提出的基于多级安全策略的强制访问控制模型(SOSACM)依然继承 BLP 模型和 Biba 模型中的严格完整性策略规则,但引入了可信度和强制约束规则来修改 Biba 模型,使保密性和完整性两个安全特性能够紧密地结合在一起. 模型中对主体和客体定义可信度则是为了防止合法的资源访问遭到拒绝.

1 安全模型的设计

1.1 模型元素

模型对系统中的每个主体分配一个访问级别,包括秘密级别 λ、完整级别 ω 和可信度. 主体的秘密级别反映了主体不将敏感信息泄露给没有持有相应允许保密级别主体的置信度,而完整级别则反映了对客体进行读、写、插入、删除和修改的置信度. 主体的可信度则反映了该主体对客体进行插入、删除和修改等操作的置信度.

相对于主体,模型对系统中的每个客体也设置一个访问级别,也包括保密级别 λ、完整级别 ω 和可信度.

这里约定 $S=\{S_1,S_2,\cdots,S_m\}$ 表示主体集合,$O=\{O_1,O_2,\cdots,O_n\}$ 表示客体集合. 可信度集合是{high, middle,low},它是全序的,即:high $>$ middle $>$low.

$P=\{P_1,P_2,\cdots,P_z\}$ 是主体能够拥有的特权集合(z 为整数). $b(s;x_1,x_2,\cdots,x_n)=\{o\mid(s,o,x_1)\in b\vee(s,o,x_2)\in b\vee\cdots\vee(s,o,x_n)\in b\}$ 表示在当前访问集合 b 中,主体 s 以 $x_1,x_2,\cdots,x_n$ 方式访问的客体的集合.

定义 1 定义模型有以下 5 种存取方式:

(1) Read(r):读包含在客体中的信息.

(2) Write(w):向客体中写信息,且允许读客体中的信息.

(3) Append(a):向客体中添加信息,且不允许读客体中的信息.

(4) Invoke(c):是主体用来授予或者撤销另外一个主体对某一个客体的访问权限的能力. 此操作仅能用于主体,使两个主体之间能够通信.

(5) Execute(e):执行一个客体(程序).

定义集合 $A=\{r,w,e,a,c\}$ 表示访问属性集.

定义 2 设 Ψ 为定义在 S 上的函数,它将 S 中的主体映射到相应的域,称 Ψ 为主体域函数. Ψ 的值域为 $\{u,v\}$,其中,u 代表普通主体域,v 代表特权主体域. $\forall g\in\Psi(S)$,记 $s_g=s\in S\mid\Psi(S)=g\}$,称 S_g 为 g 域主体集. $S=S_u\cup S_v$,其中 S_u 为普通域主体集,代表不拥有任何特权的主体集合;S_v 为特权域主体集,代表具有特权的主体集合.

同样也可以定义客体域函数.

定义 3 Φ 为定义在 S_v 上的特权映射函数,它将 S_v 中的元素映射到特权集合 P 的某个子集上,即特权映射函数的定义域是 S_v,它的值域是 $\{P_1,P_2,\cdots,P_z\}$. $\forall s\in S_v$,记 $\Phi_s=\Phi(s)$ 表示特权主体 s 所拥有的特权集合.

1.2 系统状态

定义 4 状态是系统中元素的表示形式,它由主体、客体、访问属性、访问矩阵以及标识主体和客体访问类属性的函数组成. 状态 $v\in V$ 用一个有序的四元组 $\{b,M,f,p\}$ 表示,其中:$b\in(S\times O\times A)$ 表示在某个特定的状态下,哪些主体以何种访问属性访问哪些客体,其中 S 是主体集,O 为客体集,A 是访问属性集.

$\boldsymbol{M}$ 表示访问矩阵,其中元素 $M_{ij}\subseteq A$ 表示主体 S_i 对客体 O_j 具有的访问权限集;$\boldsymbol{M}=(M_{ij})$ 为访问矩阵,表示主体 S_i 对客体 O_j 的访问方式.

$f\in F$ 表示访问类函数,记作 $F=\{f_S,f_C,f_O,f_{IS},f_{IO},f_K,f_T\}$,其中 f_S 称为主体的保密级别函数(包括主体的密级 $f_1(S)$ 和范畴 $f_3(S)$);f_C 表示主体当前保密级别函数(包括主体的密级 $f_{1c}(S)$ 和范畴 $f_{3c}(S)$);f_O 表示客体的保密级别函数(包括客体的密级 $f_2(S)$ 和范畴 $f_4(S)$). 而 f_{IS} 称为主体的完整级别函数(包括主体的重要级 $f_{I1}(S)$ 和范畴 $f_{I3}(S)$);f_{IO} 表示客体的完整级别函数(包括客体的重要级 $f_{I2}(S)$ 和范畴 $f_{I4}(S)$). f_K 称为主体的可信度函数,f_T 称为客体的可信度函数.

$p\in P$,表示主体的特权.

1.3 状态转换

系统状态间的转换由一组操作规则定义.一个规则是一个函数,它为每个状态和每个请求(输入)给出下一个状态和响应(输出).一个规则定义为函数 $\rho: R \times V \to D \times V$,其中 R 为请求的动作集,V 为状态集,D 为判定集{yes, no, error, ?},"yes"表示请求被执行,"no"表示请求被拒绝,"error"表示有多个规则适用于这一请求-状态对,"?"表示规则 ρ 不能处理此请求.$R \times V$ 是在系统中为所有请求定义的请求(request)- 状态对集合,$D \times V$ 是在系统中为所有请求定义的判定(decision) -状态对集合.在 BLP 模型中总共定义了 11 个转换规则.

系统是一安全系统,iff 系统的每一个状态 $(v_0, v_1, \cdots, v_n)$ 均为安全状态,其中 v_0 是初始状态,$v_1, \cdots, v_n$ 是其他的输出状态.

1.4 安全规则

一个系统的安全性包括保密性和完整性两个方面,因此一个系统的状态是安全的,当且仅当它满足保密性规则和完整性规则.SOSACM 模型的保密性基于 BLP 的模型,这里不再赘述,而其完整性模型则是根据 Biba 模型的严格完整性策略来定义的,描述如下.

(1) SOSACM 模型的完整性规则

公理 1　简单完整性　设 s 是 S 的一个子集,一个系统状态 $v \in (b, M, f, p)$ 满足简单完整性,iff 对任意的 $b = (s, o, x) \in B$,有 $x = r$,且 $f_{IO}(o) \geqslant f_{IS}(s)$,其中符号 $\geqslant$ 表示前者支配后者,即 $f_{I2}(o) > f_{I1}(s) \& f_{I3}(s) \supseteq f_{I4}(o)$. 简单完整性的含义是"不向下读".

公理 2　完整性 $*$ 规则　设 s 是 S 的一个子集,一个系统状态 $v \in (b, M, f, p)$ 满足完整性 $*$ 规则,iff 对任意的 $b = (s, o, x) \in B$,有:(1) $x = a$,且 $f_{IS}(s) \geqslant f_{IO}(o)$. (2) $x = w$,且 $f_{IS}(s) = f_{IO}(o)$.

完整性 $*$ 规则的含义是:当主体的完整级别支配客体的完整级别时,这体现了 Biba 模型中严格的"不向上写"的规则.

公理 3　援引规则　设 s_1, s_2 是 S 的任意两个子集,一个系统状态 $v \in (b, M, f, p)$ 满足完援引规则,iff 对任意的 $b = (s, o, x) \in B$:$x = c$,且 $f_{IS}(s_1) \geqslant f_{IO}(s_2)$.

(2) SOSACM 模型的安全规则.

公理 4　强制安全规则　将 BLP 模型所定义的保密访问控制规则[1]和公理 1、公理 2 和公理 3 所定义的完整性访问控制规则结合,SOSACM 模型有以下强制安全规则:

设 s, s_1 是 S 的任意两个子集,s' 是 S_v 的一个子集,一个系统状态 $v \in (b, M, f, p)$ 满足强制访问控制规则,iff 对任意的 $b = (s, o, x) \in B$, 有:

(1) $x = r$ 或 e,且 $(f_S(s) \geqslant f_O(o) \& f_{IO}(o) \geqslant f_{IS}(s))$ 或 $f_K(s) \geqslant f_T(o)$.

(2) $x = a$,且 $(f_S(s) \geqslant f_O(o) \& f_{IS}(s) \geqslant f_{IO}(o))$ 或 $f_K(s) \geqslant f_T(o)$.

(3) $x = w$,且 $(f_S(s) = f_O(o) \& f_{IS}(s) = f_{IO}(o))$ 或 $f_K(s) \geqslant f_T(o)$.

(4) $x = c$,且 $(f_S(s) \geqslant f_S(s_1) \& f_{IS}(s) \geqslant f_{IS}(s_1))$.

(5) $x = r, w, a$ 或 e,且 $r, w, a, e \in \Phi(s')$.

1.5 模型安全性分析

由于 SOSACM 模型的保密性安全规则基于 BLP 模型,故略去保密性安全分析.根据文献[5]中提出的自动机模型,SOSACM 模型的完整性安全分析如下.

定理 1　设自动机 G 的任意初态 v_0 满足简单完整性,则 G 满足简单完整性,当且仅当对每个变换 $(R, d, (b, M, f, p), (b^*, M^*, f^*, p^*))$,下列条件成立:(1) 每个 $(s, o, x) \in b^* - b$ 满足简单完整性;(2) 每个属于 b 但不满足简单完整性的 (s, o, x),不属于 b^*.

充分性证明如下:设 R_k 是 R 中的任意一个动作,T 为系统执行的时间.根据自动机的定义,设 (R, v, d', v') 是自动机 G 的一个变换,当且仅当存在 G 的一个执行 $\alpha = (v_0, \pi_1, v_1, \cdots)$ 和某个 $t \in T$,使得 $v_t = (d, v)$,$v_{t+1} = (d', v')$.若设 $v_0 = (b, M, f, p)$ 满足简单完整性,$\alpha = (v_0, \pi_1, v_1, \cdots)$ 是自动机 G 的一个执行,对每个 $t \in T$,令 $v_t = (b^t, M^t, f^t, p^t)$.

①证明 v_1 是安全状态.(R_1, d_1, v_0, v_1) 是 α 的一个执行片断,根据(1),每个 $(s, o, x) \in b^1 - b$ 满足简单完整性.令 $b' = \{(s, o, x) \in b \bigcup (s, o, x)$ 不满足简单完整性$\}$,根据(2),可得 $b^1 \cap b' = \varnothing$,因此若 $(s, o, x) \in b^1 \cap b$,则 (s, o, x) 必然不在 b' 中,从而 (s, o, x) 满足简单完整性.这样,任意 (s, o, x) 要么属于 $b^1 - b$,要么属

于 $b^1 \cap b$. 所以,v_1 满足简单完整性.

②证明若 v_{t-1} 满足简单完整性,则 v_t 也满足简单完整性.

重复①的证明过程,可以得到 v_t 满足简单完整规则.

必要性证明如下:使用反证法. 设 G 是一个满足简单完整性的自动机,存在某个执行片断(R_k, d_k, v_{k-1}, v_k) 使得下列条件之一成立:① 某个$(s,o,x) \in b^k - b^{k-1}$ 不满足简单完整性. ② 某个不满足简单完整性的$(s, o, x) \in b^{k-1}$,同时$(s, o, x) \in b^k$.

当①成立时,则存在某个 $(s, o, x) \in b^k$,由于 $b^k - b^{k-1} \subseteq b^k$,且$(s,o,x)$ 不满足简单完整性,所以 v_k 不满足简单完整性.

当②成立时,由于 $(s,o,x) \in b^k$,同时$(s,o,x) \in b^{k-1}$,且(s,o,x) 不满足简单完整性,所以 v_k 也不满足简单完整性,从而 G 不满足简单完整性. 这与题设矛盾. 证明完毕.

定理 2 设自动机 G 的任意初态 v_0 满足完整性 $\star$ 规则,则 G 满足完整性 $\star$ 规则,当且仅当对每个变换$(R,d,(b,M,f,p),(b^*,M^*,f^*,p^*))$,下列条件成立:

(1)对任意主体 $s \in S$,$(s,o,x) \in b^* - b$,存在 ① $x = a \Rightarrow f_{IS}^*(s) \geqslant f_{IO}^*(o)$. ② $x = w \Rightarrow f_{IS}^*(s) = f_{IO}^*(o)$.

(2)对任意主体 $s \in S$,$(s,o,x) \in b$,存在 ① 若 $x = a$ 且 $f_{IS}^*(s)\ !\geqslant f_{IO}^*(o) \Rightarrow o \notin (s,a)$. ② 若 $x = w$ 且 $f_{IS}^*(s) \neq f_{IO}^*(o) \Rightarrow o \notin (s,w)$.

用反证法可以得到证明,这里略去.

定理 3 设自动机 G 的任意初态 v_0 满足援引规则,则 G 满足援引规则当且仅当对每个变换$(R,d,(b,M,f,p),(b^*,M^*,f^*,p^*))$,对任意两个主体 $s_1 \in S, s_2 \in S$,且 $s_1 \neq s_2$,下列条件成立:(1)$(s_1,o,c) \in b^* - b \Rightarrow f_{IS}^*(s_1) \geqslant f_{IS}^*(s_2)$. (2)$(s_1,o,c) \in b$,且 $f_{IS}^*(s)\ !\geqslant f_{IS}^*(s_2)$,则 $o \notin (s_1,c)$.

证明参照定理 1 的证明方法,这里略去.

定理 4 SOSACM 的完整性安全定理

设自动机 G 具有完整性安全,当且仅当 v_0 是一个完整性安全状态,自动机 G 的每个变换 v_t 都满足定理 1、定理 2 和定理 3.

根据公理 1、公理 2、公理 3 和公理 4,显然成立.

定理 5 安全定理 一个系统是安全的,当且仅当它的每个状态都满足强制安全规则.

根据 BLP 模型,定理 4 和公理 4,显然成立.

2 结 束 语

由于基于有限状态机[6]的 BLP 模型和 Biba 模型的信息流走向完全相反,文中对主体和客体分别建立可信度策略来确保低保密级别、低完整级别的主体对高保密级别、高完整级别的客体进行插入、删除和修改等操作,以防止合法的资源访问遭到拒绝,从而把 BLP 模型和 Biba 模型有机地结合了起来,克服了以往安全模型中保密性检查和完整性检查分离的缺陷,使系统的安全性进一步得到加强,具有一定的实用性.

参考文献:

[1] Bell D E, Lapadula L J. Secure Computer Systems[R]. USA: Technical Report MTR-2457, 1973.

[2] Biba K J. Intergrity Considerations for Secure Computer Systems[R]. USA: Technical Report MTR-3153,1977.

[3] Di Vito L, Palmquist P H, Anderson E R, et al. Sepcification and Verification of the ASOS Kernel[A]. Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy[C]. Oakland: IEEE, 1990. 61-74.

[4] 蔡 谊,郑志蓉,沈昌祥. 基于多级安全策略的二维标识模型[J]. 计算机学报,2004, 27(5): 619-624.

[5] Xu Zhiwei, Bu Guanying. A Theorem on Grid Access Control[J]. 计算机科学技术学报(英文版), 2003, 18(4): 515-522.

[6] Zhang Donghong. Geometrical Significance of the Petri Net Place Invariance[J]. Journal of Xidian University, 2000, 27(6): 717-721.

(编辑:齐淑娟)