基于 Bell-La Padula 模型的三层 B 模型*)

A Three Level B Model Based on Bell-La Padula Model

管瑞峰　潘雪增　平玲娣

(浙江大学计算机科学与工程系　杭州310027)

Abstract　Bell-La Padula model is the first mandatory access control model (MAC). B model implements MAC, maintaining secrecy of system and preventing information leak. However, in practice we found that systems based on Bell-La Padula model are too restricted and lack of operability. This paper proposes the Three Level B Model, which not only implements the functions of B model, but also relaxes the access conditions. This model extends the rights of high level subjects enabling them to write downward legally on some conditions. Systems constructed beyond Three Level B Model are more practicable, and this model will be widely applied in the design of database and operating system.

Keywords　Multilevel security, Subject, Object, Access control, Mandatory access policy

1. 引言

自1967年美国国防科学委员会提出计算机安全保护问题后，1970年美国国防部(DOD)在国家安全局(NSA)建立了一个计算机安全评估中心(NCSC)，开始从事计算机安全评估的研究。1985年底，美国国防部发表了《可信计算机系统评估准则(Trusted Computer System Evaluation Criteria，缩写为TCSEC)》。根据 TCSEC 的安全评估原则，安全策略的最基本的要求是：如果某人提出获取信息的请求，则他所具备的存取类级别要大于或等于他所欲获取的存取类级别。贝尔-拉帕丢拉(Bell-La Padula)模型(以下简称 B 模型)是最早被研究的强制访问控制(MAC)模型之一，其发展过程伴随着对信息保密的军事要求，属于强制性存取控制的代表。安全策略中常把多级安全策略的模型与贝尔-拉帕丢拉模型等同视之[7]。

B 模型能够实现强制性存取控制，维护系统的保密性，有效地防止信息泄露，所以对于 B 模型的改进有很多模型，如文[6]是对于 B 模型向数据库应用方面的改进，文[4]提到的内容是将 B 模型和 Biba 模型[5]结合，增加 B 模型的完整性安全指标。这些都是对于 B 模型的访问条件进行强化以达到更加安全的目的。

但是在实践中我们发现基于 B 模型的系统有着条件过于严格的缺点，满足 * 一特性对于很多系统来说是缺乏操作性的，比如一个高级别的主体把从一个低级别的客体读出的信息写入另外一个低级别的客体中，这不是信息的泄漏，应该是合法的，可是在 B 模型中，不管主体写入低级别的信息是什么内容都是非法的，所以以上的合法操作也成了不可行的了。这是对高级别主体的过多限制以达到保护信息的目的。可是这种限制是可以避免的，为此我们在 B 模型的基础上设计了一种改进型模型——三层 B 模型，三层 B 模型继承了 B 模型现有的特点，即实现强制性存取控制，维护系统保密性，防止信息泄漏，同时又放宽了访问条件，扩展了主体的权限，使得合法的下写成为可能，基于三层 B 模型的系统将更具有实用性，它们在数据库、操作系统的设计中将有着广泛的应用。

2. Bell-La Padula 模型

B 模型的出发点是维护系统的保密性，有效地防止信息泄露，并由此描述了不同访问级别的主体和客体之间的关系。B 模型的基本思想是将存取类级别分为等级和范畴。等级是指保密的级别，在存取类中是按偏序排列的，例如：公开 < 秘密 < 机密 < 绝密。而范畴是一个集合的概念，通常是将系统内的元素根据应用的实际情况划分为若干个子集。所以范畴是相互独立的并且是无序的。范畴的例子是：导弹部队、防化兵部队、装甲部队、海军航空兵部队等。

显然，存取类是由有序的级别和无序的范畴组成的。在数学中，有序的级别称为偏序。在多级安全系统中，所有的元素(不论是主体还是客体)都被划分到不同的存取类中。存取类之间可能存在的关系有以下几种：

(1)第一存取类支配第二存取类，即其级别不低于后者，其范畴集合包含后者的全部范畴。

(2)第二存取类支配第一存取类。

(3)存取类相等，也就是上述两者都成立。

(4)上述三条均不成立，它们的存取类是互相交叉的，不能比较；第一存取类中至少有一个范畴不在第二存取类内，同时第二存取类中也有至少一个以上的范畴不在第一存取类内。

B 模型的存取规则集主要包括以下几点：

(1)*实体的划分*　计算机系统内部的实体可以分为两个抽象的集合，主体集合 S 和客体集合 O。对 S 中的每个主体 s 存在固定的安全级别 C(s)，对 O 中的每个目标存在固定的安全级别 C(o)。

(2)*简单安全特性*　是指主体只能从下读、向上写；为使主体对客体既能读又能写，二者的访问级别必须完全相同；所有的实体不能自行降级，自行降级则意味着信息有可能被泄露；最后，假如一个作为主体的进程没有对大于或等于本身密

*)项目研究得到国家自然基金资助，批准号：69884003，浙江省自然基金资助，批准号：001101352。管瑞峰　硕士生，主要研究方向为安全模型，数据库安全，操作系统安全。潘雪增　教授，博士生导师，主要研究领域为安全模型，网络信息安全，ASIC。平玲娣　教授，博士生导师，主要研究领域为安全模型，操作系统安全。

级的客体文件进行“读”，则系统允许该进程对密级小于本身密级的客体文件进行“写”。该特性的解释为，接受信息的人的安全级别必须至少跟该信息的安全级别一样高。

(3) *-特性(*-Proterty) 是指对客体 o 有“读”访问权的主体 s，仅当 C(o)<=C(p)，主体 s 可以对客体 p 有“写”访问权。该特性的解释是：得到某个级别信息的人只能把该信息向其级别不低于该信息级别的人传递。该特性防止了一个有权访问高级别数据的主体通过“写”将该数据传送给低级目标，也即防止了“下写”(Write-down)。

Bell-La Padula 模型的安全策略分为强制存取和自主存取控制两部分。强制存取包括简单的安全特性保护，要求在一给定安全级别的主体，仅被允许对同一安全级别和较低安全级别上的客体进行“读”；*-特性保护允许一给定安全级别上的主体，仅被允许向相同安全级别或较高安全级别上的客体进行“写”。

3. 改进后的三层 B 模型

针对 B 模型中对于满足 *-特性需要太严格的条件，我们提出了三层 B 模型，意在减弱满足 *-特性的条件，扩展主体的权限。下面的各种符号用语和名词术语都参见文[1～3]。

3.1 三层模型模型系统状态

我们在三层 B 模型中只讨论强制存取，不讨论自主存取。

系统状态集合 $V=P((S\times IM\times A1)\times(IM\times O\times A2))\times u\times F$，P(X)表示 X 的幂集。S 是主体集合，是系统中的主动实体，如用户。IM 是中间体集合，是系统中有主动特性也有被动特性的实体，如进程。O 是客体集合，是系统中的被动实体，如文件。A1是 S 对 IM 的访问属性集合，A1={e(执行)，r(只读)，a(只写)，w(读和写)}。A2是 IM 对 O 的访问属性集合，A2={r(只读)，a(只写)，w(读和写)}。u 是访问矩阵集，访问矩阵 M 中的元素 $M_{ij}\subseteq A$，表示 s_i 对客体 o_j 具有访问特权。F 是访问类函数集，F 中的元素记做 $f=(f_1,f_2,f_3,f_4,f_5,f_6)$，其中 $f_1(s)$ 和 $f_2(s)$ 分别表示主体 s 的密集和类别集，$f_3(im)$ 和 $f_4(im)$ 分别表示中间体 im 的密集和类别集，$f_5(o)$，$f_6(o)$ 分别表示客体 o 的密集和类别集。系统中任一状态 v=(b,M,f)，其中 $b\subseteq(S\times IM\times A1)\times(IM\times O\times A2)$ 是当前访问集。

3.2 三层模型的安全特性

(1)简单安全性：状态 v=(b,M,f)满足简单安全性 iff 对所有的 $(s,im,x_1,im,o,x_2)\in b$，(i)$x_1=e$ 或 $(x_1=a,x_2=a)$ 或 (ii)$(x_1=r,x_2=r$ 或 $x_1=w,x_2=w)$ 且 $(f_1(s)>=f_3(im),f_2(s)\supseteq f_4(im),f_3(im)>=f_5(o),f_4(im)\supseteq f_6(o))$。

(2) *'-性质：状态 v=(b,M,f)满足 *'一性质 iff 对所有的 $s\in S$，若 $b(s;w,a)!=\Phi$，且 $b(s;r,w)!=\Phi$，则 $o_1\in b(s;w,a)$，$o_2\in b(s;r,w)$ 蕴含 $f_5(o_1)\geq f_5(o_2)$ 且 $f_6(o_1)\supseteq f_6(o_2)$。

其中符号 $b(s;x_1,\cdots,x_n)$ 表示主体 s 对某具有访问特权 x_i 的所有客体 o 的集合。主体 s 对客体 o 具有访问特权 $x_i\Leftrightarrow\exists\ im\in IM$，s 对 im 有访问特权 x_i，im 对 o 有访问特权 x_i。

三层 B 模型的安全策略为强制存取，包括以上两个安全特性。简单安全特性保护要求给出了对于一定安全级别的主体只能读取低于自身级别的中间体，而一定安全级别的中间体只能读取低于自身级别的客体；*'一特性保护允许一给定安全级别上的主体，仅允许把自己能够获得的信息向相同或者较高安全级别的客体进行“写”。

3.3 三层 B 模型强制存取策略对于信息保密性的讨论

三层 B 模型对于 B 模型的最大改进在于引入了中间层的概念，能够引起读者对于该模型的保密性进行怀疑的是：主体对于中间体的执行操作是任意的。如果我们不引入主体对于中间体执行的概念，或者说我们定义主体对于中间体是不能执行的，那么我们很容易地看出来，这实际就是一个严格的只有读写操作的 B 模型：一定级别的主体只能读低级别的客体，只能写高级别的客体，只能对同级别的客体进行读写操作；只不过多了一个中间体罢了。

在引入了主体对于中间体的执行操作后，问题复杂了。不过我们可以从信息流向来讨论该三层 B 模型的保密性。我们需要保密的信息的载体为客体，信息的获得者为主体，信息流从高级别的客体流向低级别的主体或者客体，这样就是对保密性的破坏。见图1。在三层 B 模型中，这两种信息流都是非法的。

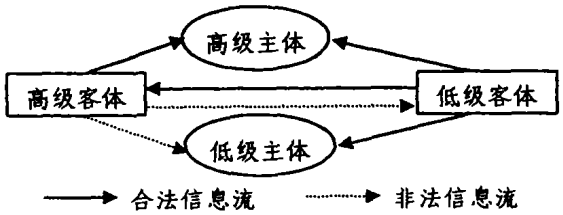

图1 信息流示意图

定理1 在三层 B 模型强制存取策略中，对于一定级别的主体 s，s 只能获得小于或等于其他级别的客体 o 的信息。

证明：设系统处于某种状态 v=(b,M,f)下，主体 s 获得了客体 o 的信息，且 $f_1(s)<f_5(o)$，$f_2(s)\subset f_6(o)$。s 获得了客体 o 的信息我们可以表示为：$o\in b(s;r,w)$，由 b(s;r,w)的定义知，存在一个中间体 im，s 对 im 有访问特权 r 和 w，im 对 o 有访问特权 r 和 w。由简单安全性得：(i)$f_1(s)>=f_3(im)$，$f_2(s)\supseteq f_4(im)$；(ii)$f_3(im)>=f_5(o)$，$f_4(im)\supseteq f_6(o)$。所以有 $f_1(s)>=f_5(o)$，$f_2(s)\supseteq f_6(o)$，这与我们的假设矛盾，所以 s 获得客体 o 的信息在三层 B 模型强制存取策略中是非法的，定理得证。

定理2 在三层 B 模型强制存取策略中，高级别客体的信息不会流入(写入)低级别的客体中。

证明：设系统处于某种状态 v=(b,M,f)下，存在这样的通道使得客体 o_1 的信息可以写入客体 o_2 中，且 $f_5(o_1)>f_5(o_2)$，$f_6(o_1)\supset f_6(o_2)$。由假设可知存在着 im_1，im_2 使得 im_1 可以对客体 o_1 进行读操作 $(f_3(im_1)>=f_5(o_1),f_4(im_1)\supseteq f_6(o_1))$，$im_2$ 可以对 o_2 进行写操作 $(f_3(im_2)>=f_5(o_2),f_4(im_2)\supseteq f_6(o_2))$。由以上可知 $f_3(im_1)>f_3(im_2)$，$f_4(im_1)\supset f_4(im_2)$(i)，即 im_1 的级别要高于 im_2 的级别，即 im_1 和 im_2 不是同一个中间体。不同的中间体之间是没有信息流的，所以存在一个主体 s，s 可对 im_1 进行读操作 $(f_1(s))>=f_3(im_1)$，$f_2(s)\supseteq f_4(im_1)$(ii))，同时对 im_2 进行写操作 $(f_1(s))<=f_3(im_2)$，$f_2(s)\subseteq f_4(im_2)$(iii))。由(i)(ii)(iii)推得 $f_1(s)<f_1(s)$，$f_1(s)\subset f_1(s)$，矛盾！所以原定理成立。

由定理1和定理2我们可以得出，三层 B 模型强制存取策略对保密信息进行了有效的保护，防止了信息的向下流失和低级别主体对高级别信息的非法获得。

3.4 三层 B 模型对 B 模型改进的讨论

从上一节我们知道三层 B 模型保持了 B 模型原有的特点，即对保密信息的保护，维护了数据的保密性。同时，该模型

和B模型相比，还增加了自己的新特点，即主体的权限扩大。在原有的B模型中为了实现数据的保密性，禁止任何形式的向下写，高级主体不能向低级客体中写任何信息，包括非高级客体中的信息。而在三层B模型中，主体通过对中间体的执行，可实现部分的下写。比如现在有高级别主体s，低级别进程im(中间体)，和与im同级别的客体文件o_1，o_2。进程im的功能是从文件o_1读取信息然后把信息写入文件o_2。那么主体s对im的执行最终导致的结果是向低级别文件中写入了同级别的信息，这种对数据的写入不会造成任何高级信息的下漏。所以说我们的三层B模型是在保持数据保密性的前提下对B模型的改进，扩充了B模型中主体的权限，即高级别主体可以向低级别客体中写入低级别的信息，所以这个模型更具有实用性。改进示意图如图2。

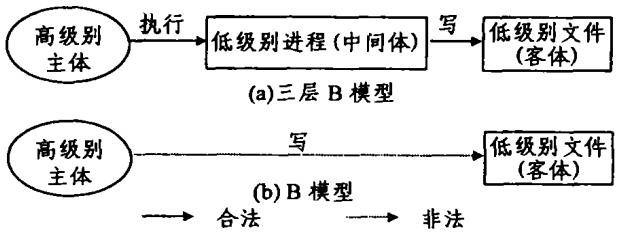

图2　三层B模型和B模型比较图

4. 三层B模型的应用展望

因为三层B模型具有的新特点，将使得它在数据库，操作系统的设计中有着广泛的使用前景。这个模型尤其适合使用在操作系统的设计中，在操作系统的设计中，用户将承担主体的角色，进程将承担中间体的角色，而各种文件将是客体。用户对于进程的读写将成为进程对于输出设备的输出和获得输入设备的数据，而进程对于文件的读写则是一般概念上的读写，用户对于进程的执行也是一般概念上的执行。中间体的数目随着进程的创建，结束而变化。于是整个对于客体文件的读写都由作为中间体的进程完成，主体用户要对客体文件进行读写操作时，都必须通过运行相应进程(如果用户运行一个执行文件，那么他运行后产生的进程的级别就是这个执行文件的级别)，由进程把读到的信息输出给主体用户(即输出到输出设备上)，这样完成主体用户的读；用户把输入信息输入到输入设备中，再由进程读取，这样完成主体用户的写。当低级别的主体用户需要把信息写入低级别的客体文件时，他可以把这个权限赋予给高级别的主体用户，即编写相应写入文件进程(这个进程必须没有对输入输出设备的读写)，把该进程交给高级别主体用户执行，这样就完成了高级别主体用户向低级别客体文件写入信息的过程，值得我们注意的是，这时高级别主体写入的内容是低级别的内容而不是高级别客体中的内容，所以没有造成高级别信息的泄漏。同时当高级别的主体用户需要把高级别主体文件中的信息写入同级别的客体文件时，他也可以编写一个读写进程(该进程也不能有对输入输出设备的读写，否则低级别的客体用户就不能运行)交给低级别的主体用户执行。

当然，这个模型也会有自己不完善的地方，它应用于操作系统可能还需要改进，但是对于大多数基于B模型的操作系统来说，将其建立成基于三层B模型的操作系统，将是一件非常有意义的事情。

参考文献

1 Bell D E, La Padula L J. Secure Computer System: Mathematical Foundations. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol I, 1973

2 Bell D E, La Padula L J. Secure Computer System: a Mathematical Model. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol II, 1973

3 Bell D E, La Padula L J. Secure Computer System: a Refinement of the Mathematical Model. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol III, 1973

4 Sandhu R S. Lattice-based access control models. Computer, 1993,26(11):9～19

5 Biba K J. Integrity Considerations for Secure Computer Systems, The Mitre Corporation, Bedford, MA, April 1977

6 洪帆，蔡蔚，余详宣. 一个用于多级安全关系数据库系统的改进Bell-La Padula模型. 计算机学报，1995,18(10):763～769

7 杨智慧. 计算机信息系统安全技术. 北京：群众出版社，1998

(上接第118页)

(a)　(b)　(c)

图5　(a)Lena原图　(b)阈值T0=0.35时的分类图
(c)阈值T0=0.60时的分类图

隶属度值U的大小还可以作为该点嵌入水印强度系数，以实现自适应水印嵌入。具体应用FCM聚类算法的数字水印方案，我们将在后续工作中予以报道。

参考文献

1 Cox I J, Killian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for images, audio and video. In: Pro. IEEE ICIP (Int. Conf. on Image Processing), Lausane, Switzerland, 1996. 243～246

2 Hsu C-T, Wu J-L. Hidder signature in images. In: Proc of ICIP, 1996. 223～226

3 O'Ruanaidh J, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking [J]. Signal Processing, 1998, 66(3): 303～317

4 Der-Chyuan LOU, Te-Lung YIN. Adaptive digital watermarking using fuzzy clustering technique. IEICE trans. fundamentals, 2001, E84-A(8)

5 Jain A K, Dubes R C. Algorithms for Clustering Data. Prentice Hall, 1988

6 Murty M N, Jain A K. Knowledge-based Clustering Schema for Collection Management and Retrieval of Library Books. Pattern Recognition, 1995, 28(7)

7 Shortland R, Scarfe R. Digging for Gold (Data Management). IEE Review, 1995, 41 (5): 213～217

8 Han J. Conference tutorial notes: Data Mining Techniques. In: Proc. of ACM SIGMOD Intl. Conference' 96 on Management of Data (SIGMOD' 96). Montreal, Canada, June 1996