基于格的 BLP 完整性扩展模型

沈 瑛[1,2]，沈昌祥[1,3]
(1. 浙江大学 计算机学院，杭州 310027；2. 浙江工业大学 计算机学院，杭州 310023；
3. 北京工业大学 计算机学院，北京 100124)

摘 要： 为了扩展 BLP 模型融入完整性，并解决 BLP 与 Biba 模型典型融合中的高保密完整性资源与低保密完整性资源互访困难问题，从数学背景乘积格角度分析 BLP 模型，构造了 BLP-I 扩展模型. BLP-I 模型中标签的第 2 维分量改为可信级别，通过突出保密性中读操作和完整性中写操作的地位，区分主体和已读信息的可信级，协调了在生命周期内 BLP 模型的静态特性和 Biba 模型的动态特性. BLP-I 模型以低保密完整性下级可向高保密完整性上级直接汇报，而上级主体可下调自身安全级间接向下级发指令的方式部分解决了互访困难问题.

关键词： 访问控制；信息系统；安全系统
中图分类号： TP 303 **文献标志码：** A **文章编号：** 0254 - 0037(2013)03 - 0402 - 05

BLP Integrity Expansion Model on Lattice

SHEN Ying[1,2], SHEN Chang-xiang[1,3]
(1. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China;
2. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China;
3. College of Computer Science, Beijing University of Technology, Beijing 100124, China)

Abstract: Mutual access dilemma between double-high level and double-low level resources in security and integrity was usually appeared during BLP model expansion with Biba. BLP model expansion with integrity which could resolve this dilemma was represented. An expansion model named BLP-I model was constructed in the view of product lattice analysis since lattice was BLP's mathematical background. The second dimension of label in BLP-I was substituted to indicate trust level. Read operation in security attribute and write operation in integrity were highlighted. The trust level of subject and messages had been read were distinguished. So the tranquility in BLP and dynamics in Biba during a lifecycle were coordinated in BLP-I. At last, dilemma was partially solved in BLP-I by permitting low security and integrity level direct report to double-high level while permitting double-high level lowered its own security level to issue to its underling.

Key words: access control; information systems; security systems

TCSEC[1]、CC[2]和 GB/T 22239—2008[3]等标准中对重要信息系统都采用强制访问控制策略，侧重安全保密性的 BLP 模型[4]是其中核心的访问控制模型. 在重要系统、物联网和云等新环境的建设中，访问控制策略除了安全保密，还需要融合完整性，而侧重完整性的 Biba 模型[5]因为结构相似往往成为与 BLP 模型融合的首选；但直接融合 2 个模型会面临高保密完整性级别的资源与低保密完整性级

收稿日期： 2011-08-14.
基金项目： 国家科技重大专项基金资助项目(2010ZX01037-001-001)；国家软科学研究计划资助项目(2010GXQ5D317)；浙江省重点科技创新团队基金资助项目(2009R50009).
作者简介： 沈 瑛(1976—)，女，副教授，主要从事信息安全、虚拟现实方面的研究，E-mail: shenying@zjut.edu.cn.

别资源间被禁止访问的问题，而这样的访问控制策略将拒绝军政等重要系统中上级与下级间通信的正常需求. 本文提出了一个融合完整性要求的 BLP 扩展模型来解决这一困境，并从乘积格的角度分析了模型的有效性.

1　BLP 模型

1.1　BLP 模型基本表述

BLP 模型把系统描述为由于主客体之间的访问请求和决策导致的状态转换. 它基于系统安全的公理性假设：若系统满足自主安全属性、简单安全(SS)条件和星(*)属性，则是安全的. 自主安全要求系统的每个访问请求都在访问控制矩阵内，属于自主访问控制. 简单安全条件指主体未经授权不能读取高安全级的敏感信息，防止泄密. 星属性主要防止主体间接泄漏信息给客体，如防止木马进程通过复制敏感文件并写到其他文件中传递信息.

BLP 模型中形式化相关的符号有：主体集合 S、客体集合 O、安全等级集合 C、请求集合 R、访问控制矩阵 M、个体分类集合 K 和安全标签等. 其中 S 和 O 常指向系统中的进程、文件等. C 中等级一般为未分级 U、机密 C、秘密 S、绝密 TS，依次递增. 请求 R 一般指只读 r、只写 a 和读写 w. 主客体安全标签可用二元组 $\langle f, g\rangle$ 表示. 其中第 1 个分量 f 表示安全级，具体可用 f_o、f_c 和 f_s 分别表示客体的安全等级、主体当前安全等级和主体的最高安全等级；第 2 个分量表示为可操作的对象范围，g 是 K 的子集.

可定义辅助标记：支配 $\uparrow$ 和主体 s 请求访问的客体集合 $b(s: q_1, \cdots, q_n)$ 为

$$\langle a_1, b_1\rangle \uparrow \langle a_2, b_2\rangle = a_2 \geqslant a_1 \wedge b_2 \supseteq b_1$$

$$b(s: q_1, \cdots, q_n) = \{o \mid o \in O \wedge [(s, o, q_1) \in b \vee \cdots \vee (s, o, q_n) \in b\}, b \subseteq S \times O \times R$$

利用上述符号，BLP 模型可以表示如下.

1) 自主安全属性　$\forall(s, o, q) \in S \times O \times R$ 必有 $q \in M[s, o]$.

2) SS 条件　$\forall(s, o, q) \in (S \times O \times R)$ 当且仅当：

$-\forall o \in b(s: \mathrm{r}, \mathrm{w}) \Rightarrow \langle f_o(o), g(o)\rangle \uparrow \langle f_s(s), g(s)\rangle$

3) * 属性　$\forall(s, o, q) \in (S \times O \times R)$ 满足 * 属性当且仅当：

$-\forall o \in b(s: \mathrm{a}) \Rightarrow \langle f_c(s), g(s)\rangle \uparrow \langle f_o(o), g(o)\rangle$

$-\forall o \in b(s: \mathrm{r}) \Rightarrow \langle f_o(o), g(o)\rangle \uparrow \langle f_c(s), g(s)\rangle$

$-\forall o \in b(s: \mathrm{w}) \Rightarrow \langle f_o(o), g(o)\rangle = \langle f_c(s), g(s)\rangle$

1.2　BLP 模型的格解读

BLP 模型的构造立足于格[6]. 本文从格的视角来分析并扩展 BLP 模型. 格 $\langle A, \wedge, \vee\rangle$ 是任意元素对都有上下确界的偏序关系. BLP 模型对应了元素为二元组的乘积格.

1) 构造格. BLP 其实是由线序的 C 和幂集 $P(K)$ 构成的乘积格 $\langle C \times P(K), \wedge, \vee\rangle$，格中元素为安全标签 $\langle f, g\rangle$. 运算 $\wedge$ 和 $\vee$ 为 $\langle f_j, g_l\rangle \wedge \langle f_k, g_m\rangle = \langle \min(f_j, f_k), g_l \cap g_m\rangle$；$\langle f_j, g_l\rangle \vee \langle f_k, g_m\rangle = \langle \max(f_j, f_k), g_l \cup g_m\rangle$. 当元素对满足 $\langle f_1, g_1\rangle \uparrow \langle f_2, g_2\rangle$ 时，标签 $\langle f_2, g_2\rangle$ 是上确界，$\langle f_1, g_1\rangle$ 是下确界.

2) 格元素映射. 客体以标签 $\langle f_o(o), g(o)\rangle$ 映射到格中，简记为 l_o，主体分别以当前标签 $\langle f_c(s), g(s)\rangle$ 和最高标签 $\langle f_s(s), g(s)\rangle$ 映射到格中，分别简记为 l_c 和 l_s.

3) 规则映射. 因为 $\forall x \in F(x) \Leftrightarrow F(y)$，客体自由变量遍历 SS 条件、* 属性中的客体，简化表示如下.

SS 安全条件当且仅当：

$$\mathrm{r}, \mathrm{w} \Rightarrow l_o \uparrow l_s$$

* 属性当且仅当：

$$a \Rightarrow l_c \uparrow l_o; \mathrm{r} \Rightarrow l_o \uparrow l_c; \mathrm{w} \Rightarrow l_c = l_o$$

可以看到，BLP 乘积格中只有自下向上的访问请求才可以通过，即“上写、下读”策略. BLP 模型通过在一定时间段内校正主体当前安全标签，判断格上的主客体标签对是否可比、信息流动是否向上，来完成请求决策和系统状态动态变迁. 格模型便于从静态角度分析 BLP 模型下的系统行为，同时表明合理分配主客体标签是实施 BLP 模型的关键.

2　BLP-I 扩展模型

BLP 模型成功地表达了保密性策略，高安全要求的重要系统往往会以它为基础构建访问控制策略，但由于 BLP 缺乏对完整性的约束且标签的第 2 个分量涉及集合幂运算，使可能的标签数呈指数增长. 本文提出一个 BLP-I 扩展模型，融入完整性、取代幂运算，以迎合系统建设需求.

完整性相关访问控制模型有 Biba、Lipner、Clark-Wilson 等. Biba 以外的其他模型多从商业环境出发，结构差异较大，很难融入到 BLP 模型，因

此,BLP 模型的完整性扩展一般以 Biba 为基础[7-8]. 其中 Biba 的严格完整性策略与 BLP 结构最接近,在各自维度上读写方向恰好相反,两者直接复合为乘积格后,〈高保密性,高完整性〉与〈低保密性,低完整性〉的标签对不可比较,即不允许实际中保密性和完整性较高的上级访问下级,下级也无法向上级汇报,不利于系统实施. 文献[7]引入可信主体提高了可用性,但需要重新审视可信主体的引入是否改变了原模型的安全和完整性假设等.

BLP-Ⅰ扩展模型的特色主要体现在以下 3 点.

第一,区别对待读、写请求. 由于一旦违背 BLP 模型,必然有低等级向高等级直接或间接的"上读",然后才可能写信息引起泄露,所以 BLP 中读比写更关键;而 Biba 侧重防范信息篡改,则写操作远比读操作危险[5]. 基于此,在 BLP-Ⅰ模型中细分了读支配、写支配分别应对保密性和完整性.

第二,BLP-Ⅰ模型的完整性度量设计. 事实上主体、进程、数据信息的完整性指标一直存在着可信、可靠等差异[9]. BLP-Ⅰ模型中采用可信度等级刻画主客体的完整性,并增加主体当前已读信息的最低可信级来区分主体自身的可信度与主体已掌握信息的可信度. 在 BLP-Ⅰ模型中标签的第 2 个分量由原来的个体分类集合替换成可信级别,把原分量的子集操作外置. 这样,BLP-Ⅰ模型的标签对应的二元分量都呈线性递增(减),标签数量大大减小,尤其方便了系统间互联、扩展.

第三,BLP-Ⅰ模型的策略设计. 扩展模型把原操作范围集合判断移入自主安全条件判断中,以保持 BLP 模型对主客体操作范围的控制. BLP-Ⅰ模型的完整性策略是 Biba 低水印策略的变形. 低水印策略允许主体读任意级别的客体,但每次读后调整主体可信度,主体只能向级别不超过它本身的客体写,只能执行级别不超过它本身的主体. 由于该策略简单可靠,已在不少多级系统中采纳,但是随着多次读将导致主体可信级别下降,不断减小主体可下写的范围. 即使通过可信操作干预上调主体可信级别,也仍然存在频繁调整的问题且可能破坏完整性假设. BLP-Ⅰ模型把低水印策略改为:主体可以读任意可信级别的客体;主体进行读操作后不改变自身的可信级,但会影响当前已读信息的最低可信级;主体只能向下写,要求客体的可信级别不超过主体自身的可信级以及主体当前已读信息的最低可信级别. 该变形基于以下事实:完整性要规避高可信度信息被低级信息篡改,信息的可信度应该建立在写操作的主体本身可信度和该主体读入信息的可信度上,可以取两者中的较低者. 因而,主体读入不同可信度的信息只需要反映在主体已读信息的最低可信度上,而不必影响主体本身的可信度. 这种处理区分了主体可信度和主体所读信息的可信度 2 个不同概念.

3 BLP-Ⅰ模型形式化

类似 BLP,BLP-Ⅰ模型也可以形式化,采用符号有主体集合 S、客体集合 O、主客体安全等级集合 C、请求集合 R、访问控制矩阵 M、个体分类集合 K 和标签等. 新引入了可信度等级集合 I,其典型的可信度级别有可信级、系统级、应用级、用户级、不可信级,依次递减. 标签为二元组 $\langle f, g\rangle$,2 个分量分别对应个体的安全和可信度级别. 其中第 1 分量 f 同 BLP 模型,分为 f_o, f_c, f_s;扩展模型中第 2 分量 g 也有 3 种模式:g_o, g_I, g_s,分别表示客体的可信等级、主体当前已读信息的最低可信等级和主体的可信等级,g_I初值为最高可信级别. 引入 k_o、k_s,分别表示主客体各自的操作范围,是 K 的子集.

BLP-Ⅰ模型结合保密性、完整性,可以类似给出系统安全的公理性假设. 定义:若系统满足自主安全属性、简单安全(SS′)条件、简单完整性(SI)条件和星(* ′)属性,则是安全的. 其中除了增加新的约束外,SS′条件和* ′属性也相应有所变化.

定义新的支配↑′,类似地可构造一维的读支配↑$_f$、写支配↓$_g$:

$$\langle a_1, b_1\rangle \uparrow' \langle a_2, b_2\rangle = a_2 \geqslant a_1 \wedge b_2 \leqslant b_1$$

$$\langle a_1, b_1\rangle \uparrow_f \langle a_2, b_2\rangle = a_2 \geqslant a_1$$

$$\langle a_1, b_1\rangle \downarrow_g \langle a_2, b_2\rangle = b_2 \leqslant b_1$$

其中后 2 个运算可以看作是第 1 个运算的投影.

1) 自主安全属性 $\forall(s,o,q) \in S \times O \times R$ 必有 $q \in M[s,o]$ 且

$$-\forall o \in b(s:\mathrm{a}) \Rightarrow k_s \subseteq k_o$$

$$-\forall o \in b(s:\mathrm{r}) \Rightarrow k_o \subseteq k_s$$

$$-\forall o \in b(s:\mathrm{w}) \Rightarrow k_o = k_s$$

2) SS′条件 $\forall(s,o,q) \in (S \times O \times R)$ 当且仅当:

$$-\forall o \in b(s:\mathrm{r},\mathrm{w}) \Rightarrow f_s(s) \geqslant f_o(o)$$

3) SI 条件 $\forall(s,o,q) \in (S \times O \times R)$ 当且仅当:

$$-\forall o \in b(s:\mathrm{a},\mathrm{w}) \Rightarrow g_s(s) \geqslant g_o(o)$$

4) * ′属性 $\forall(s,o,q) \in (S \times O \times R)$ 当且仅当:

$$-\forall o \in b(s:\mathrm{a}) \Rightarrow \langle f_c(s), g_I(s)\rangle \uparrow' \langle f_o(o), g_o(o)\rangle$$

$-\forall o \in b(s:\mathrm{r}) \Rightarrow \langle f_o(o), g_o(o)\rangle \uparrow_f \langle f_c(s), g_I(s)\rangle$ and $g_I(s) := \min(g_I(s), g_o(o))$

$-\forall o \in b(s:\mathrm{w}) \Rightarrow f_c(s) = f_o(o)$ and $\langle f_c(s), g_I(s)\rangle \downarrow_g \langle f_o(o), g_o(o)\rangle$

BLP-I 模型中简单安全条件和简单完整性条件用于阻止直接违背安全和完整性需求的访问请求，而星属性公式用于否决间接违背安全和完整性需求的访问请求. 主体当前已经读取信息的最低可信等级通过初值和操作从主体最高可信度向下调整，作用类似于保密性中的主体当前安全级别的指标，只是它具有动态性而后者在当前访问周期中是静态的. 同时随着主体读操作，主体当前已读取信息的可信度逐渐降低直至最低点，但不影响其基于保密性的向下读和向上写. 这体现了 BLP-I 模型是以 BLP 为主的模式，即 BLP-I 模型保持了 BLP 模型主客体在生命周期内的静态特性和 Biba 的动态特性，又避免了 Biba 模型低水印策略由于主体可信级别下降导致的不可访问问题.

4　BLP-I 格解释和示例

BLP-I 模型定义了代数系统 $\langle C \times I, \wedge', \vee'\rangle$，元素用二元组 $\langle f_i, g_j\rangle$ 表示，其中：$f_i \in C$; $g_j \in I$. C 沿用 BLP 中安全级分量，采用可信度级别作为完整性集合 I. 运算 $\langle f_j, g_l\rangle \wedge' \langle f_k, g_m\rangle = \langle \min(f_j, f_k), \max(g_l, g_m)\rangle$; $\langle f_j, g_l\rangle \vee' \langle f_k, g_m\rangle = \langle \max(f_j, f_k), \min(g_l, g_m)\rangle$. 当 $\langle f_1, g_1\rangle \uparrow' \langle f_2, g_2\rangle = f_2 \geqslant f_1 \wedge g_2 \leqslant g_1$ 时，$\langle f_2, g_2\rangle$ 是元素对的上确界，$\langle f_1, g_1\rangle$ 是下确界. 代数系统 $\langle C \times I, \wedge', \vee'\rangle$ 元素间关系为相互不可支配、支配、被支配.

显然新代数系统 $\langle C \times I, \wedge', \vee'\rangle$ 运算 $\wedge'$ 和 $\vee'$ 关于集合 $C \times I$ 封闭，由于内部运算 min、max 本身可交换、可结合、相互可吸收，故运算 $\wedge'$ 和 $\vee'$ 也满足交换律、结合律，彼此满足吸收律，也构成了格 $\langle C, \min, \max\rangle$ 和格 $\langle I, \max, \min\rangle$ 复合成的乘积格. 因此，格中任意元素对最大下界和最小上界分别对应运算 $\wedge'$ 和 $\vee'$，所以 BLP-I 模型仍对应乘积格. BLP-I 模型对应的哈斯图以安全级递增为默认方向，也说明扩展模型中 BLP 是主导的.

BLP-I 模型仍可把自主安全条件作为静态特性在格元素映射前完成检查，客体以标签 $\langle f_o(o), g_o(o)\rangle$ 映射到格上，主体对应最高标签 $\langle f_s(s), g_s(s)\rangle$ 和主体当前已读信息标签 $\langle f_c(s), g_I(s)\rangle$ 映射到格中的 2 个元素.

以{U，C，S，TS} 安全级和{可信级、系统级、应用级、用户级、不可信级} 递减可信级可构成 BLP-I 格，如图 1 所示. 为便于表示，图中以整数 1 ~ 5 表示可信度，5 是最高级. 图中可以看到支配对应格中元素对的可比性，如元素 a 支配 b，说明 a 和 b 可比，且 a 是上确界，b 是下确界. 虚线提示安全级别与可信级别高低反向，对应上写下读的保密性要求与下写的完整性要求在方向上相反. 新引入的读支配 $\uparrow f$、写支配 $\downarrow g$ 各自刻画了乘积格中只考虑第 1、2 个分量得到的一维特性，类似投影操作. 读支配 $\uparrow f$ 时，操作相当于把乘积格 $\langle C \times I, \wedge', \vee'\rangle$ 投影后退回到 $\langle C, \min, \max\rangle$ 线性格. BLP-I 偏重 BLP 的保密安全性，读支配比写支配更重要.

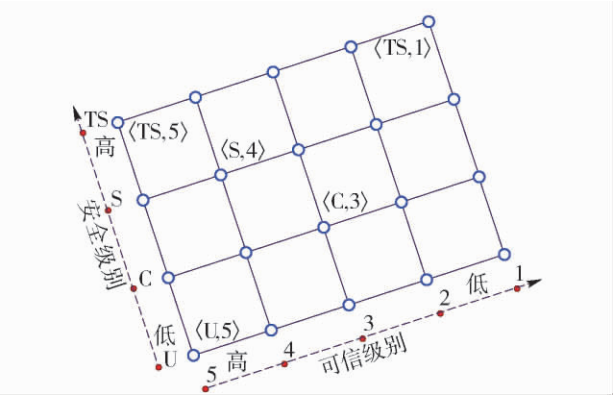

图 1　BLP-I 模型对应的乘积格

Fig. 1　Product lattice corresponding to BLP-I

在 BLP-I 格中简单安全条件(SS′)、简单完整性条件和星(*′)属性规则简化为判断对应的主客体格元素间访问产生的信息流是否与格的方向和附加的一维格一致.

图 1 中，如果某主体当前标签 $\langle f_c(s), g_I(s)\rangle$ 对应格元素 ⟨S，4⟩，主体最高标签 $\langle f_s(s), g_s(s)\rangle$ 对应元素 ⟨TS，5⟩，当前要访问的某客体对应元素 ⟨C，3⟩，访问请求为只读，则从格中可判断允许该主体读客体. 因为 TS > C 满足简单安全条件、S > C 满足星属性，本访问请求不涉及简单完整性条件. 本次访问后主体的当前标签改为 ⟨S，3⟩，表明由于本次读操作，主体的数据信息可信度下降. 当然，若主体需访问多个客体，则需遍历各客体对应的所有格元素. 本例中信息从 C 级流向 S 级符合模型要求，如格中代表主客体的 2 个元素在格中二维或一维上相互不可比较或者流动方向为负，则系统拒绝请求.

BLP-I 模型中读操作只要求主体当前安全级不低于客体(安全级下读)，不检查可信度. 写操作 a 则既检查主体当前安全级不超过客体(安全级上

写)，又检查主体当前可信度不低于客体(可信度下写)，即 BLP-I 中读只需监测安全级一维，而写操作检查二维. 模型中信息向上流动比向下输出容易，即泄露检查比完整性检查更严格，因此，BLP-I 模型在强调保密性基础上融合了完整性.

如果有一下级主体 s_1(当前标签为〈U,1〉，最高标签为〈C,1〉，$k_{s_1}=\{a,b\}$)要向上级 s_2 主体(当前标签为〈S,4〉，最高标签为〈TS,5〉，$k_{s_2}=\{a,b,c\}$)汇报客体 o(标签为〈C,1〉，$k_o=\{a,b\}$)，则格中可建立信息流为：s_1〈U,1〉写 o〈C,1〉、s_2〈S,4〉读 o〈C,1〉被接受，因为 $s_1 \uparrow o$，$o \uparrow_f s_2$. 反之，上级 s_2 受* ′属性制约不能下写.

由示例可知，BLP-I 支持下级主体向上级汇报的信息流〈低安全，低可信〉下级写〈高安全，低可信〉客体，然后〈高安全，高可信〉上级读该客体. 同时，BLP-I 禁止上级向下级直接发布命令以防止敏感信息泄露. 信息流中〈高安全，高可信〉主体写〈高安全，任意可信〉客体被允许，但下级主体〈低安全，低可信〉在读取该客体时因违背星(* ′)属性而被禁止了，即针对 BLP 与 Biba 融合中的上下级通信困难，BLP-I 模型允许“下级向上级汇报”但不支持“上级向下级直接发布指令”. 上级可在下一生命周期下调自身的当前安全级与下级的当前级相同，对应〈高安全，高可信〉主体借助〈低安全，高可信〉的临时身份按安全级分批向〈低安全，低可信〉下级主体发布命令. 应该说下级向上级的汇报作为信息汇集过程，仅供上级参考，允许开放是可行的，而上级向下级直接发布命令是信息泄露的高危操作，容易被木马进程等利用，BLP-I 模型有必要拒绝此类直接访问；因而，BLP-I 为解决重要系统中上下级信息正常流通的困难给出了可行的方案.

5 结论

1) 运用乘积格数学工具理解 BLP 模型，构建了融合 Biba 的扩展模型 BLP-I 模型. 扩展模型在保密性维度上侧重读操作，在完整性维度上则侧重写操作.

2) BLP-I 模型部分解决了 BLP 和 Biba 复合模型中低保密完整性与高低保密完整性主体间互访困难的典型问题. BLP-I 模型中低保密完整性的下级可向高保密完整性上级汇报，上级主体可下调自身的安全级间接向下级发布指令.

参考文献：

[1] Department of Defense of US. Trusted computer system evaluation criteria (TCSEC) [R]. Washington, D. C.: Department of Defense of US, 1985.

[2] CCMB. Common criteria for information technology security evaluation V3. 1 [R]. Washington, D. C.: Common Criteria Maintenance Board, 2006.

[3] 全国信息安全标准化技术委员会. GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求 [S]. 北京：中国标准出版社，2008.

[4] BELL D E, LaPADULA L J. Secure computer systems: mathematical foundations (MITRE 2547) [R]. Bedford: Mitre Corporation, 1973.

[5] BIBA K J. Integrity considerations for secure computer systems (MITRE 3153) [R]. Bedford: Mitre Corporation, 1977.

[6] SANDHU R. Lattice-based access control models [J]. IEEE Computer, 1993, 26(11): 9-19.

[7] 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.
CAI Yi, ZHENG Zhi-rong, SHEN Chang-xiang. A planar attributes model based on multi level security policy [J]. Chinese Journal of Computers, 2004, 27(5): 619-624. (in Chinese)

[8] 段立娟，刘燕，沈昌祥. 一种多安全域策略支持的管理机制 [J]. 北京工业大学学报，2011，37(4)：609-613.
DUAN Li-juan, LIU Yan, SHEN Chang-xiang. Management mechanism for multi-domain strategy [J]. Journal of Beijing University of Technology, 2011, 37(4): 609-613. (in Chinese)

[9] 卿斯汉，沈昌祥. 高等级安全操作系统的设计 [J]. 中国科学 E 辑：信息科学，2007，37(2)：238-253.
QING Si-han, SHEN Chang-xiang. An improved dynamically modified confidentiality policies model [J]. Science in China Series E: Information Sciences, 2007, 37(2): 238-253. (in Chinese)

(责任编辑 梁 洁)