动态多级安全系统安全标记的格模型

谭 良[1]，罗 讯[2]，周明天[2]

(1. 四川师范大学电子工程学院 成都 610066; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】分析了安全标记的概念，给出了安全标记的形式化定义，并建立了动态多级安全标记的格模型理论。格模型理论回答了动态多级安全系统的安全标记集合在数学上应形成格，解决了两安全标记比较时上、下确界的存在性问题，为多级安全性从静态安全政策，通过该策略的历史敏感性特征转化为动态安全政策奠定了理论基础。

关 键 词 标记; 动态多级安全; BLP(Bell LaPadula)安全模型; 多安全政策; 格

中图分类号 TP309 文献标识码 A

Lattice Model of Secure Labels for Dynamic Multi-Level Security System

Tan Liang[1]，Luo Xun[2]，Zhou Mingtian[2]

(1. School of Computer Science and Engineering, UEST of China Chengdu 610054;
2. College of Electronic Engineering, Sichuan Normal University Chengdu 610066)

Abstract Conception of secure labels is analyzed, and defined by formalization, subsequently the lattice model theory of labels for dynamic multi-level security is established, which shows that the set of secure labels for dynamic multi-level security comes into being “lattice order” in math, and solves the existence of g.l.b and l.u.b when one secure label compares to other, and establishes the theoretical basis for change from static multi-level security to dynamic multi-level security according to the history sensitivity.

Key words label; dynamic multi-level security; BLP security model; multi-security policies; lattice

在常规的多级安全(Multi-Level Security，MLS)系统实现中[1, 2]，进程(主体)的当前安全标记一旦确定之后，在进程的整个生存期内是不会改变的[3]。但无论采取什么方法，在给进程的当前安全标记赋值时，很难预测进程以后的资源访问行为，所赋的值极有可能无法满足合法的资源访问要求。文献[4，5]提出了一种新的MLS实施策略(A New Enforcement Approach of BLP, A-BLP)，文献[6]提出了安全标记通用架构(Security Label Common Framework, SLCF)，允许系统根据进程活动的实际场景对当前安全标记进行合理的动态调整，以解决赋值不准确和合法访问受拒绝的问题，使得MLS策略呈现出动态特征。本文仅以A-BLP为例展开讨论。

A-BLP是以BLP政策模型的公理2为中心构造的[7]。按照A-BLP策略，在进行安全判定时，除了以主体的当前安全标记$f_C(S)$和客体的安全标记$f_O(O)$为依据以外，还要考虑L_{RH}和L_{WL}这样的历史因素。L_{RH}和L_{WL}表示的是在一个进程生存期间的两个判定参考量，它们反映了以前的授权对安全标记的影响情况。L_{RH} 的初值为系

收稿日期：2003 – 02 – 20
基金项目：国家863计划资助项目(863-104-03-01)
作者简介：谭 良(1973 –)，男，现为电子科技大学在读博士生，主要从事信息安全、中间件方面的研究.

统最小安全标记值，L_{WL} 的初值为系统最大安全标记值。随着进程活动的推进，L_{RH} 的值由最大下界函数g (L_{RH}, $f_O(O)$)确定，而L_{WL}的值由最小上界函数l (L_{WL}, $f_O(O)$)确定。函数g 、l的值依赖两个安全标记的相互关系。在动态MLS中，主、客体安全标记有何特征、在数学上形成什么关系、任意的两个安全标记是否存在最大下界和最小上界，本文将讨论这些问题。

1　安全标记

安全标记包括类别和范畴两个部分。类别部分反映出来的是一种等级关系，故又称为安全等级；范畴部分由无等级的元素组成，表示一清晰的信息领域。无等级是指不存在一范畴“大于”另一范畴，正如不能说“红色”大于或小于“蓝色”一样。在经典的BLP模型中，安全标记具有“全局性”和“永久性”特征。换句话说，在强制访问控制多级安全策略中，无论何时何地，主、客体的安全标记是不会改变的。这一特征在多级安全系统中称为“宁静性原则”。对于一个具体的访问控制策略而言，如果它具有以上两项特征，那么其标记的集合在数学上必然会形成“偏序关系”[8, 9]。

2　安全标记的格模型理论

如果通过改变MLS的实施策略来达到动态性，主体安全标记是否仍然按“偏序关系”构造呢？从A-BLP和SLCF可以看出，主体安全标记之间的关系仅仅是“偏序关系”，还不能保证函数g、l有解，而历史敏感性的改变又严格依赖这两个函数，因此本文通过建立安全标记的格模型理论来解决函数g、l的解的存在性问题。

2.1　安全标记的格模型

定理 1　$\underline{C}$ 是等级分类集合，$\underline{K}$是范畴类别集合，在集合$\underline{C}$上定义一运算“$\leq$”表示等级元素的“小于等于”关系，代数系统($\underline{C}$，$\leq$)是一个偏序集；在集合$\underline{K}$上定义一个运算“$\subseteq$”，表示范畴集合中的包含关系，代数系统($\underline{K}$，$\subseteq$)也是一个偏序集。

证明　$\forall x \in \underline{C}$，$x \leq x$，所以$\underline{C}$中的元素具有反身性；$\forall x,y \in \underline{C}$, 如果 $x \leq y$，$y \leq x$，则$x=y$，所以$\underline{C}$中的元素具有反对称性；$\forall x, y, z \in \underline{C}$, 如果 $x \leq y$，$y \leq z$，则 $x \leq z$，所以$\underline{C}$中的元素具有传递性，由定义1可得，代数系统($\underline{C}$，$\leq$)是一个偏序集。同理可得代数系统($\underline{K}$，$\subseteq$)也是一个偏序集。证毕。

定义 1　$\underline{C}$、$\underline{K}$是非空集合，把$\underline{C}$、$\underline{K}$的笛卡儿积 $\underline{C} \times \underline{K}$ 称为安全标记L，记为L:={(C，K)| $C \in \underline{C} \wedge K \in \underline{K}$}。

定义 2　L_{MIN}是系统的最小安全标记值，L_{MAX}是系统的最大安全标记值，显然有$L_{\mathrm{MIN}} \in L$，$L_{\mathrm{MAX}} \in L$。

定理 2　设$\leq$是安全标记集合L上的运算，规定 (C_1，K_1) $\leq$ (C_2，K_2)，当且仅当 $C_1 \leq C_2$, $K_1 \subseteq K_2$，$C_1, C_2 \in \underline{C}$，$K_1, K_2 \in \underline{K}$，则($L$，$\leq$)作成一个格。

证明　1) 首先证明(L，$\leq$)是一个偏序关系。$\forall$ (C_1，K_1)$\in L$，由于 $C_1 \leq C_1$，$K_1 \subseteq K_1$，则 (C_1，K_1) $\leq$ (C_1，K_1)，所以L中的元素具有反身性；$\forall$ (C_1，K_1)，(C_2，K_2)$\in L$，如果 (C_1，K_1) $\leq$ (C_2，K_2)，(C_2，K_2) $\leq$ (C_1，K_1)，有$C_1 \leq C_2$，$C_2 \leq C_1$，$K_1 \subseteq K_2$，$K_2 \subseteq K_1$ 得 $C_1=C_2$，$K_1=K_2$，则 (C_1，K_1) = (C_2，K_2)，所以L中的元素具有反对称性；$\forall$ (C_1，K_1)，(C_2，K_2)，(C_3，K_3)$\in L$，如果(C_1，K_1) $\leq$ (C_2，K_2)，(C_2，K_2) $\leq$ (C_3，K_3)，有$C_1 \leq C_2$，$C_2 \leq C_3$，$K_1 \subseteq K_2$，$K_2 \subseteq K_3$ 得$C_1 \leq C_3$，$K_1 \subseteq K_3$，则(C_1，K_1) $\leq$ (C_3，K_3)，所以L中的元素具有传递性；由定义1得L是一个偏序集。

2) 其次证明L中的任意两个元素存在最大下界(greatest lower bound, g.l.b)。$\forall$ (C_1，K_1)，(C_2，K_2)$\in L$，按如下方式构造另一元素(C_3，K_3)，分两种情况证明。

(1) 如果C_1 ! $\leq$ C_2 且 C_2 ! $\leq$ C_1 或 K_1 ! $\subseteq$ K_2 且 K_2 ! $\subseteq$ K_1，规定 (C_3，K_3) = g.l.b{ (C_1，K_1)，(C_2，K_2)}= L_{MIN}。

(2) 如果$C_1 \leq C_2$，则 $C_3 = C_1$，否则 $C_3 = C_2$；如果 $K_1 \subseteq K_2$，则 $K_3 = K_1$，否则 $K_3 = K_1 \bigcap K_2$；那么，显然就有 (C_3，K_3) $\in L$。

对于情况(1)，得到的(C_3，K_3) 也是 (C_1，K_1)，(C_2，K_2) 的最大下界，结论成立。

对于情况(2)，首先证明按情况(2)构造的(C_3，K_3) 是 (C_1，K_1)，(C_2，K_2) 的下界。如果C_1 !$\leq$ C_2，即

$C_1 > C_2$，则 $C_3 = C_2$，所以有$C_3 \leq C_2 < C_1$，即$C_3 \leq C_1$，$C_3 \leq C_2$，就有当$C_1 ! \leq C_2$ 时

$$C_3 \leq C_1 \text{ 且 } C_3 \leq C_2 \tag{1}$$

如果 $C_1 \leq C_2$ ，则 $C_3 = C_1$，所以有$C_3 = C_1 \leq C_2$，即$C_3 \leq C_1$，$C_3 \leq C_2$，就有当$C1 \leq C2$ 时

$$C_3 \leq C_1 \text{ 且 } C_3 \leq C_2 \tag{2}$$

如果$K_1 ! \subseteq K_2$，有$K_3 = K_1 \bigcap K_2$ ，而 $K_1 \bigcap K_2 \subseteq K_1$，$K_1 \bigcap K_2 \subseteq K_2$，即有$K_3 \subseteq K_1$ 、$K_3 \subseteq K_2$，就有当 $K_1 ! \subseteq K_2$ 时

$$K_3 \subseteq K_1 \text{ 且 } K_3 \subseteq K_2 \tag{3}$$

如果 $K_1 \subseteq K_2$，则 $K_3 = K_1$，有 $K_3 = K_1 \subseteq K_2$，即 $K_3 \subseteq K_1$，$K_3 \subseteq K_2$，就有当 $K_1 \subseteq K_2$ 时

$$K_3 \subseteq K_1 \text{ 且 } K_3 \subseteq K_2 \tag{4}$$

根据式(1)、(2)、(3)和(4)知，在各种情况下，总有 $C_3 \leq C_1$，$C_3 \leq C_2$，$K_3 \subseteq K_1$ ，$K_3 \subseteq K$，即 $(C_3, K_3) \leq (C_1, K_1)$ 且 $(C_3, K_3) \leq (C_2, K_2)$，所以，$(C_3, K_3)$ 是 (C_1, K_1) 和 (C_2, K_2) 的下界。

下面证明(C_3, K_3) 是(C_1, K_1) 和(C_2, K_2) 的最大下界。设(C_4, K_4) 是(C_1, K_1) 和 (C_2, K_2) 的任意一个下界，则有$C_4 \leq C_1$ ，$C_4 \leq C_2$ ，$K_4 \subseteq K_1$，$K_4 \subseteq K_2$。而C_3 的取值是C_1 或C_2，无论取哪一个值，都有

$$C_4 \leq C_3 \tag{5}$$

而 $K_4 \subseteq K_1 \bigcap K_2$ ，但 K_3 的取值是 K_1 或 $K_1 \bigcap K_2$，无论取哪一个值，都有

$$K_4 \subseteq K_3 \tag{6}$$

结合式(5)和(6)可知

$$(C_4, K_4) \leq (C_3, K_3) \tag{7}$$

前面已经证明(C_3, K_3)，(C_1, K_1) 和(C_2, K_2) 的下界，而(C_1, K_1) 和(C_2, K_2) 的任意一个下界(C_4, K_4)，都有式(7) 成立，所以(C_3, K_3) 是 (C_1, K_1) 和 (C_2, K_2) 的最大下界。

综合情况(1)和(2)可得，L中的任意两个安全标记的最大下界是存在的。

3) 证明L中的任意两个元素存在最小上界(least upper bound, l.u.b)。$\forall (C_1, K_1), (C_2, K_2) \in L$，按如下方式重新构造元素$(C_3, K_3)$，分两种情况：

(1) 如果$C_1 ! \leq C_2$ 且$C_2 ! \leq C_1$或$K_1 ! \subseteq K_2$ 且$K_2 ! \subseteq K_1$，规定$(C_3, K_3) = \text{l.u.b}\{(C_1, K_1), (C_2, K_2)\} = L_{MAX}$；

(2) $C_1 ! \geq C_2$，$C_3 = C_2$，否则 $C_3 = C_1$；如果 $K_1 ! \supseteq K_2$，则 $K_3 = K_1 \bigcup K_2$，否则 $K_3 = K_1$，显然$(C_3, K_3) \in L$。

证明L中的任意两个元素存在最小上界的过程与2)相似，限于篇幅，证明过程略。所以L中的任意两个安全标记的最小上界是存在的。

综合情况1)、2)和3)，由定义2可知$(L, \leq)$是一个格，证毕。

定理 3 $(L, \leq)$是一个有界格。

证明 对于任给的$L_1 \in L$，有$L_1 \vee L_{MIN} = L_{MIN}$，$L_1 \wedge L_{MAX} = L_{MAX}$，所以 L_{MIN} 和L_{MAX} 是格 $(L, \leq)$的泛下界和泛上界，所以$(L, \leq)$是一个有界格。证毕。

值得注意的是，在证明定理2的过程中，当 (C_1, K_1) 和 (C_2, K_2) 没有关系时，构造的 (C_3, K_3) 分别是 L_{MIN} 和L_{MAX}。这样的构造并不影响A-BLP和SLFC的实施，因为如果 (C_1, K_1) 和 (C_2, K_2) 没有关系，它们已被排除在实施算法之外。但这样的构造可以保证证明过程的严密性和理论完备性，因而是合理的。

2.2 安全标记格模型的意义

按照定理2 构造的安全标记可以满足动态多级安全系统，此类安全标记的全景视图如图1。从图1可以看出，在A-BLP中，L_{RH} 的初始值为 L_{MIN}，而L_{WL} 的初始值为 L_{MAX}。

建立动态多级安全系统安全标记的格模型理论具有重要的理论意义和实际意义，主要表现在以下3个方面：

1) 经典BLP模型的静态MLS仅要求安全标记具有“全局性”和“永久性”特征，要求主、客体的安全标记无论何时何地不能改变，在数学上形成偏序关系；具有历史敏感性的动态MLS的客体安全标记特点与

静态MLS相同，但主体安全标记与静态MLS不同，具有“全局性”和“动态性”，即主体安全标记在不违反安全原则的条件下可以进行合理的调整，在数学上形成格。

2) 动态多级安全标记的格模型理论可以保证函数g、l解的存在性，具有重要的理论意义。

3) 定理2 既是一个证明过程，又是一个构造过程，定理4 告诉我们如何构造动态MLS的主体安全标记，具有重要的实际意义。

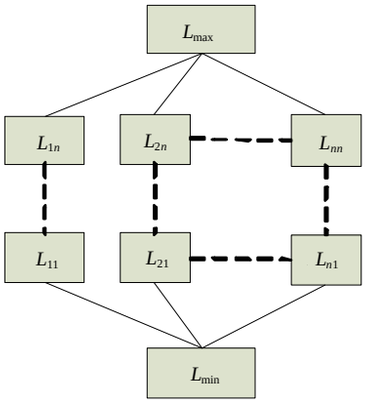

图1　安全标记的格模型

3　结 束 语

安全标记是实现多级安全系统的基础，是实施强制访问控制策略的前提。本文分析了当前国内外安全系统的安全标记实施情况，给出了安全标记的形式化定义，并建立了安全标记的格模型理论。格模型理论回答了动态MLS的安全标记集合在数学上应形成格，解决了两安全标记比较时上、下确界的存在性问题，为多级安全性从静态安全政策，通过实施强制访问控制策略的历史敏感性特征转化为动态安全政策奠定了理论基础。

参 考 文 献

[1] Branstad D. Data categorization and labeling (executive summary)[C]. In: Proceedings of the 13th National Computer Security Conference, Washington: NIST Press, 1990. 32-33

[2] George F, Meade G. Department of defense trusted computer system evaluation criteria[S]. department of defense computer security center, M D 20755, 1983. 382-443

[3] Gligor V D, Chandersekaran C S, Chapman R S, *et al*. Design and implementation of secure Xenix[J]. IEEE Transactions on Software Engineering, 1987, SE-13(2): 208-221

[4] 石文昌, 孙玉芳, 梁洪亮. 经典BLP安全公理的一种适应性标记实施方法及其正确性[J]. 计算机研究与发展, 2001, 38(11): 1 366-1 372

[5] 石文昌, 孙玉芳. 多级安全政策的历史敏感性[J]. 软件学报, 2003, 14(1): 91-96

[6] 梁洪亮, 孙玉芳, 赵庆松. 一个安全标记公共框架的设计与实现[J]. 软件学报, 2003, 14(3): 547-552

[7] Bell D E, Lapadula L J. Secure computer systems: unified exposition and multics interpretation[J]. MITRE Corp, 1976, MTR: 2 997-3 130

[8] Secure Computing Corporation. DTOS generalized security policy specification[C]. Technical Report, No.DTOS-CDRL-A019, Secure Computing Corporation, 1997. 285-362

[9] 刘克龙. 安全Linux操作系统及安全Web系统的形式化建模与实现[D]. 北京: 中国科学院软件所, 2001

编　辑　熊思亮