第35卷 第21期 计 算 机 工 程 2009年11月
Vol.35 No.21 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)21—0171—03 文献标识码：A 中图分类号：TP311.5

基于扩充敏感标记的格理论模型研究

马新强[1]，黄 羿[1]，李丹宁[2]
(1. 重庆文理学院计算机学院，重庆 402160；2. 贵州科学院，贵阳 550002)

摘 要：为在实现多级安全系统过程中有效兼顾BLP模型与Biba模型，分析安全模型敏感标记集合在数学上形成的格理论，提出一种能够有效融合这些模型的敏感标记格安全理论模型，以同时标识信息机密性与完整性，通过构建新的敏感标记格理论模型，为信息安全模型研究提供一定的理论依据。

关键词：安全模型；格；敏感标记；BLP模型；Biba模型

Research on Lattice Theoretical Model Based on Extended Sensitivity Label

MA Xin-qiang[1], HUANG Yi[1], LI Dan-ning[2]
(1. College of Computer, Chongqing University of Arts and Sciences, Chongqing 402160; 2. Guizhou Academy of Sciences, Guiyang 550002)

【Abstract】 In order to give attention to BLP model and Biba model in process of implementing multi-level security system, the lattice theory shaped in math of security model sensitivity labels sets is analyzed. A security theoretical model of sensitivity labels lattice is proposed, which can fuse these two models. The information confidentiality and integrity are labeled. By setting up new sensitivity labels lattice theoretical models, the theory basis is provided to information security research.

【Key words】 security model; lattice; sensitivity label; BLP model; Biba model

1 概述

系统安全是整个计算机安全的基础，信息系统的安全性主要体现在3个方面：机密性(保密性)，完整性和可用性。机密性是指防止计算机中的信息泄露，即信息只能被合法的用户所见，而不能被非授权的用户获得；完整性指计算机中的信息不能被非法进行修改或破坏；可用性指系统能有效地提供必要的服务，即能对计算机资源进行预期的有效管理。

在计算机信息系统中，为保障信息的机密性、完整性和可用性，对信息的访问和操作，一般需要遵循一定的安全策略。只有当所有的用户只能按照安全策略所授权的方法进行信息的操作，信息系统才是安全的，而敏感标记是实现多级安全系统的基础，是实施强制访问控制安全策略[1]的前提。安全模型是对安全策略所表达的安全需求的简单、抽象和无歧义的描述。BLP模型[2]只考虑信息的机密性，而Biba模型[3]只考虑完整性。只有把机密性与完整性有机的结合起来，才能更好地满足信息的可用性要求。文献[4]对保密性的敏感标签做了形式化分析，但完整性涉及较少；文献[5]在每个具体的任务中保持机密性和完整性的局部一致。目前，还没有出现两者兼顾的敏感标记的安全模型。因此，研究和设计两者兼顾的敏感标记安全模型理论具有重大意义。

2 经典安全模型分析

2.1 BLP模型

BLP模型[2]是常用的一种计算机多级安全模型。BLP模型的安全策略包括2部分：自主安全策略(DAC)和强制访问控制策略(MAC)[6]。文献[2]描述了BLP模型是个状态机模型，并形式化地定义了系统、系统状态以及系统状态间的转换规则及安全概念，并制定一组安全特性，以此对系统状态和状态转换规则进行限制和约束，使得对于一个系统而言，如果它的初始状态是安全的，并且所经过的一系列规则转换都保持安全，那么可以证明该系统是安全的。在模型中用 f 表示主、客体的敏感级别，BLP关于读写关系控制的规则特性如下：

(1)简单安全特性：主体 s 能够读客体 o 必须满足：
$f(o) \le f(s)$

(2)星(*)特性：主体 s 能够写客体 o 必须满足：
$f(s) \le f(o)$

简单安全特性保证主体对客体的“不能上读”，而星(*)特性保证主体对客体的“不可下写”。这2个特性控制信息只能在同级之间或从低级向高级流动，形成的敏感标记 f 在偏序小于等于下构成一个格，既下读 $f(o) \le f(s)$ 或等价于 $f(o) \to f(s)$，上写 $f(s) \le f(o)$ 或等价于 $f(s) \to f(o)$。但是这种信息流只是从保密性角度考虑的，没有涉及信息的完整性问题。

2.2 BiBa模型

Biba模型[4]是仿照BLP模型构造的，类似于BLP模型中的访问类结构，定义每个完整性类由完整性级和信息类(既受保护的对象)组成，实际上是由完整性集合与信息类集合的乘积形成的。同时，Biba模型仿造BLP模型，在完整性类之

基金项目：国家自然科学基金资助项目(90718009)；贵州省高新技术发展及产业化基金资助项目(黔科合成字[2008]5014号)；重庆文理学院校内科研基金资助项目(Z2008SJ15, Y2007SJ43)
作者简介：马新强(1979－)，男，讲师、硕士，主研方向：信息安全，形式化方法；黄 羿，讲师、硕士；李丹宁，研究员、博士
收稿日期：2009-06-20 **E-mail：**mxq345@sohu.com

间定义了关系 $\le$，描述完整性类之间的支配关系，并使它符合偏序关系和格的要求。

模型中也同样定义了严格完整性信息流控制策略：简单完整性特性和完整性*特性。假设安全系统中包括主体集合 S 和客体集合 O，对于 S 中的每个主体 s 和 O 中的每个客体 o，它们的完整性级分别记做 $I(s)$ 和 $I(o)$，则 2 条特性描述如下：

(1)简单完整性特性：如果主体 s 可以读客体 o，则

$I(s) \le I(o)$

(2)完整性*特性：如果主体 s 对具有完整性 $I(o)$ 的目标有写的访问权限，则

$I(o) \le I(s)$

这 2 条性质严格防止了低完整性级别的主体对信息的修改。这 2 个特性控制信息只能在同级之间或从高完整级向低完整级流动，形成的敏感标记 I 在偏序≤下构成一个格，既上读 $I(s) \le I(o)$ 或等价于 $I(s) \to I(o)$，下写 $I(o) \le I(s)$ 或等价于 $I(o) \to I(s)$。

Biba 模型注重信息的完整性，防止低完整性信息破坏高完整性信息，忽略了信息的保密性，BLP 模型则相反。实际系统中往往需要同时兼顾完整性和保密性 2 个方面，目前还没有同时兼顾满足这两者要求的统一的形式模型。

3 扩充的敏感标记安全模型

扩充的敏感标记模型涉及完整性和保密性 2 个方面，下面给出其定义，并加以证明，最终才能形成一种基于扩充敏感标记的格理论安全模型。

定义 1 设 $\langle L, \le \rangle$ 是偏序集，如果 $\forall x, y \in L$，且 $\{x, y\}$ 在 L 中都有最小上界和最大下界，那么就称 L 关于偏序小于等于构成一个格。

定义 2 三元组 $L = (C, I, K)$，其中，$L = \{L_1, L_2, \cdots, L_p\}$ 为敏感标记即 $C \times I \times K$ 的笛卡儿积的集合；$C = \{C_1, C_2, \cdots, Cq\}$ 是保密级分类集合；$I = \{I_1, I_2, \cdots, Iq\}$ 是完整密级分类集合；$K = \{K_1, K_2, \cdots, K_r\}$ 是范畴分类集合。

定理 1 集合 $C = \{C_1, C_2, \cdots, Cq\}$，$I = \{I_1, I_2, \cdots, Iq\}$，在 C 与 I 上分别定义运算“ $\le$ ”表示密级元素的“小于等于”关系，代数系统 $(C, \le)$ 与 $(I, \le)$ 分别是一个偏序集；$K = \{K_1, K_2, \cdots, K_r\}$ 在集合 K 上定义运算“ $\subseteq$ ”表示范畴集合中的包含关系，代数系统 $(K, \subseteq)$ 也是个偏序集。

证明 因为 $\forall x \in C$，$x \le x$，所以 C 中的元素具有自反性；$\forall x, y \in C$，如果 $x \le y$，$y \le x$，则 $x = y$，所以，C 中的元素具有反对称性；$\forall x, y, z \in C$，如果 $x \le y$，$y \le z$，则 $x \le z$，所以，C 中的元素具有传递性，所以，代数系统 $(C, \le)$ 是个偏序集。同理可得代数系统 $(I, \le)$ 与 $(K, \subseteq)$ 也是个偏序集。

定义 3 $L_{\min}$ 是系统的最小安全敏感标记值，$L_{\max}$ 是系统的最大安全敏感标记值，有 $L_{\min} \in L$，$L_{\max} \in L$。

定理 2 设“ $\le$ ”表示敏感标记集合 L 上的运算，有 $(C_1, I_1, K_1)(C_2, I_2, K_2) \Leftrightarrow (C_1 \le C_2, I_1 \le I_2, K_1 \subseteq K_2)$，$C_1, C_2 \in C$，$I_1, I_2 \in I$，$K_1, K_2 \in K$，则 $(L, \le)$ 形成一个格。

证明 首先证明 $(L, \le)$ 是个偏序关系。根据自反性：$\forall (C_1, I_1, K_1) \in L$，由 $C_1 \le C_1, I_1 \le I_1, K_1 \subseteq K_1$，则 $(C_1, I_1, K_1) \le (C_1, I_1, K_1)$，所以，$L$ 中的元素具有反身性；反对称性：$\forall (C_1, I_1, K_1), (C_2, I_2, K_2) \in L$，如果 $(C_1, I_1, K_1) \le (C_2, I_2, K_2)$，$(C_2, I_2, K_2) \le (C_1, I_1, K_1)$，有 $C_1 \le C_2$，$C_2 \le C_1$，$I_1 \le I_2$，$I_2 \le I_1$，$K_2 \subseteq K_1$，得 $C_1 = C_2$，$I_1 = I_2$，$K_1 = K_2$，则 $(C_1, I_1, K_1) = (C_2, I_2, K_2)$，所以，$L$ 中的元素具有反对称性；传递性：$\forall (C_1, I_1, K_1)(C_2, I_2, K_2)(C_3, I_3, K_3) \in L$，如果 $(C_1, I_1, K_1) \le (C_2, I_2, K_2)$，$(C_2, I_2, K_2) \le (C_3, I_3, K_3)$，有 $C_1 \le C_2$，$C_2 \le C_3$，$I_1 \le I_2$，$I_2 \le I_3$，$K_1 \subseteq K_2$，$K_2 \subseteq K_3$，得 $C_1 \le C_3$，$I_1 \le I_3$，$K_1 \subseteq K_3$，则 $(C_1, I_1, K_1) \le (C_3, I_3, K_3)$，所以，$L$ 中的元素具有传递性；再由定义 2 得 L 是个偏序集。

其次证明 L 中的任意 2 个元素存在最大下界(Greatest Lower Bound, GLB)。

$\forall (C_1, I_1, K_1), (C_2, I_2, K_2) \in L$，按如下方式构造另一元素 (C_3, I_3, K_3)，分 2 种情况证明。

(1) 如果 $C_1 ! \le C_2$ 且 $C_2 ! \le C_1$，$I_1 ! \le I_2$ 且 $I_2 ! \le I_1$ 或 $K_1 ! \subseteq K_2$ 且 $K_2 ! \subseteq K_1$，规定 $(C_3, I_3, K_3) = GLB\{(C_1, I_1, K_1), (C_2, I_2, K_2)\} = L_{\min}$。

(2)如果 $C_1 \le C_2$，$I_1 \le I_2$，则 $C_3 = C_1$，$I_3 = I_1$，否则 $C_3 = C_2$，$I_3 = I_2$；如果 $K_1 \subseteq K_2$，则 $K_3 = K_1$，否则 $K_3 = K_1 \cap K_2$；那么，显然就有 $(C_3, I_3, K_3) \in L$。

对于情况(1)，得到的 (C_3, I_3, K_3) 是 (C_1, I_1, K_1)，(C_2, I_2, K_2) 的最大下界，结论成立。

对于情况(2)，需证明(2)构造的 (C_3, I_3, K_3) 是 (C_1, I_1, K_1)，(C_2, I_2, K_2) 的下界。如果 $C_1 ! \le C_2$，$I_1 ! \le I_2$，即 $C_1 > C_2$，$I_1 > I_2$，则 $C_3 = C_2$，$I_3 = I_2$，所以，有 $C_3 \le C_2 < C_1$，$I_3 \le I_2 < I_1$，即 $C_3 \le C_1$，$C_3 \le C_2$，$I_3 \le I_1$，$I_3 \le I_2$，那么当 $C_1 ! \le C_2$，$I_1 ! \le I_2$ 时，可以得到：

$$C_3 \le C_1 \text{且} C_3 \le C_2, I_3 \le I_1 \text{且} I_3 \le I_2 \quad (1)$$

如果 $C_1 \le C_2$，$I_1 \le I_2$，则 $C_3 = C_1$，$I_3 = I_1$，所以，有 $C_3 = C_1 \le C_2$，$I_3 = I_1 \le I_2$，即 $C_3 \le C_1$，$C_3 \le C_2$，$I_3 \le I_1$，$I_3 \le I_2$，那么当 $C_1 \le C_2$，$I_1 \le I_2$ 时，可以得到：

$$C_3 \le C_1 \text{且} C_3 \le C_2, I_3 \le I_1 \text{且} I_3 \le I_2 \quad (2)$$

如果 $K_1 ! \subseteq K_2$，有 $K_3 = K_1 \cap K_2$，而 $K_1 \cap K_2 = K_1$，$K_1 \cap K_2 = K_2$，即有 $K_3 \subseteq K_1$，$K_3 \subseteq K_2$，那么当 $K_1 ! \subseteq K_2$ 时，可以得到：

$$K_3 \subseteq K_1 \text{且} K_2 \subseteq K_3 \quad (3)$$

如果 $K_1 \subseteq K_2$，则 $K_3 = K_1$，有 $K_3 = K_1 \subseteq K_2$，即 $K_3 \subseteq K_1$，$K_3 \subseteq K_2$，那么当 $K_1 \subseteq K_2$ 时，可以得到：

$$K_3 \subseteq K_1 \text{且} K_2 \subseteq K_3 \quad (4)$$

根据式(1)~式(4)可知，在各种情况下，总有 $C_3 \le C_1$ 且 $C_3 \le C_2$，$I_3 \le I_1$ 且 $I_3 \le I_2$，$K_3 \subseteq K_1$ 且 $K_2 \subseteq K_3$，即 $(C_3, I_3, K_3) \le (C_1, I_1, K_1)$ 且 $(C_3, I_3, K_3) \le (C_2, I_2, K_2)$，所以，$(C_3, I_3, K_3)$ 是 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的下界。

下面证明 (C_3, I_3, K_3) 是 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的最大下界。设 (C_4, I_4, K_4) 是 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的任意一个下界，则有 $C_4 \le C_1$，$I_4 \le I_1$，$C_4 \le C_2$，$I_4 \le I_2$，$K_4 \subseteq K_1$，$K_4 \subseteq K_2$，而 C_3 的取值是 C_1 或 C_2，无论取哪一个值，都有：

$$C_4 \le C_3, I_4 \le I_3 \quad (5)$$

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

$$K_4 \le K_3 \quad (6)$$

结合式(5)和式(6)可知：

$$(C_4, I_4, K_4) \le (C_3, I_3, K_3) \quad (7)$$

前面已经证明 (C_3, I_3, K_3) 是 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的下界，而 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的任意一个下界 (C_4, I_4, K_4)，都有式(7)成立，所以，(C_3, I_3, K_3) 是 (C_1, I_1, K_1) 和 (C_2, I_2, K_2) 的最大下界。

综合上述可得，L 中的任意 2 个安全标记的最大下界是

存在的。

接下来证明 L 中的任意 2 个元素存在最小上界(Least Upper Bound, LUB)。

$\forall(C_1,I_1,K_1),(C_2,I_2,K_2)\in L$，按如下方式重新构造元素 (C_3,I_3,K_3)，分 2 种情况：

(1) 如果 $C_1!\le C_2$ 且 $C_2!\le C_1$，$I_1!\le I_2$ 且 $I_2!\le I_1$ 或 $K_1!\subseteq K_2$ 且 $K_2!\subseteq K_1$，规定 $(C_3,I_3,K_3)=LUB\{(C_1,I_1,K_1),(C_2,I_2,K_2)\}=L_{\max}$。

(2)当 $C_1!\ge C_2$，$I_1!\ge I_2$，否则 $C_3=C_1$，$I_3=I_1$；如果 $K_1!\supseteq K_2$，则 $K_3=K_1\cup K_2$，否则 $K_3=K_1$，显然 $(C_3,I_3,K_3)\in L$。证明 L 中的任意 2 个元素存在最小上界的过程与上述过程相似，限于篇幅，证明过程略。所以，L 中的任意 2 个安全标记的最小上界是存在的。

因此，可以知道 $(L,\le)$ 是一个格。

定理 3 $(L,\le)$ 是个有界格。

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 $(L,\le)$ 的泛下界和泛上界，所以，$(L,\le)$ 是个有界格。

在证明定理 2 的过程中，当 (C_1,I_1,K_1) 和 (C_2,I_2,K_2) 没有关系时，构造的 (C_3,I_3,K_3) 分别是 $L_{\min}$ 和 $L_{\max}$。这样的构造可以保证证明过程的严密性和理论完备性。

通过证明可知扩充的敏感标记集合在数学上形成了格的模型理论。

4 安全性分析

从对信息流模型、BLP 模型和 Biba 模型的安全性分析可以看出，主体对客体信息的访问主要是根据其敏感标记的来确定信息的流动方向，若从 BLP 模型和 Biba 模型两者同时考虑信息流动方向，就能同时保证其机密性与完整性问题。本模型信息的流动方向主要是根据敏感标记来区分的，这样在对敏感标记进行扩充下，既包括保密标记 f，又包括完整标记 I。当用户按照本安全策略所授权的方法进行信息的操作，同时保证其机密性与完整性，证明信息系统是安全的。扩充的敏感标记集合在数学上应形成格，保证了模型的严密性。

5 结束语

本文根据 BLP 模型和 Biba 模型的敏感标记集合扩充形成新的敏感标记的格理论模型，融合 2 种模型的优点，对信息安全性得到加强，为研究动态安全策略奠定了理论基础。本文模型已在 LogicSQL 安全数据库系统中加以实施，尤其是在企业搜索中将得以应用。下一步研究工作是在此扩充的敏感标记格理论的基础上形成新的安全模型，并对其进行动态的安全性分析。

参考文献

[1] Osbom S. Mandatory Access Control and Role-based Access Control Revisited[C]//Proc. of the 2nd ACM Workshop on Role-based Access Control. Virginia, USA: ACM Press, 1997.

[2] Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations[R]. MITRE Corporation, Tech. Rep.: MTR-2547, 1973.

[3] Biba K. Integrity Considerations for Secure Computer Systems[R]. Air Force Electronic Systems Division, Tech. Rep.: 76-372, 1977.

[4] 马新强, 王保华, 李丹宁, 等. 一种形式化的强制访问控制模型的研究与实现[J]. 计算机研究与发展, 2006, 43(S1): 284-288.

[5] 赵　勇, 刘吉强, 韩　臻, 等. 基于任务的访问控制模型研究[J]. 计算机工程, 2008, 34(5): 28-30.

[6] Denning D E. A Lattice Model of Secure Information Flow[J]. Comm. ACM, 1976, 19(5): 236-243.

编辑　陈　文

（上接第 170 页）

从表 2、表 3 可以看出，对于几何攻击，本文算法的鲁棒性比文献[4]方法更强，对于内容不同的图像在经过攻击后，水印的检测率是不同的，但是绝大部分图像都可以成功检测。在实验过程中发现，当图像经过缩放变换或是裁切等各种攻击后，图像的一些特征点会发生偏移或去除，但是这并不影响水印的提取检测。

5 结束语

本文提出一种可以有效抵抗一般性几何攻击的公钥数字图像水印算法，以 SIFT 特性为基础，在特征点区域上实现水印的嵌入和提取检测。

实验结果表明，该算法具有以下几个优点：

(1)特征点提取对于几何攻击具有不变性，这对水印的鲁棒性有很大提高；

(2)水印信息通过密钥随机地嵌入到所选区域中，保证了水印的安全性；

(3)采用公钥水印策略，私钥用于水印信息的提取，公钥用于水印的检测，私钥水印对于抗公钥攻击也有较高的鲁棒性。

由此可见，本文所提出的方法具有一定理论和实用价值。

参考文献

[1] Bas P. Geometrically Invariant Watermarking Using Feature Points[J]. IEEE Transactions on Image Processing, 2002, 11(8): 825-840.

[2] Lee H Y. Robust Image Watermarking Using Local Invariant Features[J]. Optical Engineering, 2006, 45(3): 1931-1934.

[3] 刘向丽, 寇卫东, 王志国. 一种抗几何攻击的公钥水印算法[J]. 西安电子科技大学学报, 2007, 34(4): 629-633.

[4] 孙　鑫, 易开祥, 石教英, 等. 公开钥数字水印系统研究[J]. 计算机辅助设计与图形学报, 2003, 15(7): 875-879.

[5] Lowe D G. Distinctive Image Features From Scale Invariant Key Points[J]. International Journal of Computer Vision, 2004, 60(2): 91-110.

编辑　陈　文