安全计算机系统的 Bell-LaPadula 形式化模型*)

The Bell-LaPadula Formal Model for Secure Computer Systems

王贵林　卿斯汉　倪惜珍　冯登国

(中国科学院软件研究所信息安全国家重点实验室　北京100080)

(中国科学院信息安全技术工程研究中心　北京100080)

Abstract　In this paper, the Bell-LaPadula formal model for secure computer systems is introduced, and the key theoretical results are proved. In addition, we also point out that the sufficient and necessary condition, given by reference[11], for secure information system is wrong. Exploiting a new concept, the correct sufficient and necessary condition is presented.

Keywords　Information security, Secure computer systems, Bell-LaPadula formal model, Formal analysis

一、引言

著名的 Bell-LaPadula 形式化模型(简称为 BLP 模型)是由 MITRE 公司的 Bell 和 LaPadula 在文[1～3]中提出的，随后被广泛用于形式化地描述和证明计算机系统的安全[4～10]。文[11]给出了信息保密系统的 Bell-LaPadula 模型的形式化描述，并证明了几个结论。其中一个重要的结论就是，判断信息系统是否为保密系统的充分必要条件。但我们发现，该结论的证明是错误的。事实上，文[11]给出的只是一个充分条件，而不是必要条件。另外，文[12]将 Bell-LaPadula 作了修改和扩充，得到了一个新的修改 BLP 模型，并成功地将修改后的模型用于设计 SecLinux 安全操作系统。但文[12]并没有给出修改 BLP 模型的形式化证明。

借助于一个新的概念-动作(action)，我们给出了在 Bell-LaPadula 形式化模型下，计算机系统安全的充分必要条件。同时，本文还对 Bell-LaPadula 形式化模型中的主要结果作了证明。另外，需要指出的是，虽然安全模型的根本是首先要给出主体、客体和访问属性三元组的安全性满足条件的概念(即本文的定义4)，但本文中的所有形式化定理却不依赖于该定义的具体含义。这样，尽管本文的定义4和文[11]所给出的定义略有差别，但由此导致的两个模型下的主要理论结果仍然是相同的。

本文介绍 BLP 模型；给出 BLP 模型中的主要结论；最后是总结。

二、安全计算机系统的 Bell-LaPadula 模型

安全计算机系统的 Bell-LaPadula 模型中的元素有：主体、客体、密级、范畴、访问属性、请求、决定、控制矩阵、系统状态、状态序列等。给定任意集合 G 和 H，我们用 G^+ 表示集合 $G\cup\{\phi\}$(ϕ 为空集)，用 $P(G)$ 表示 G 的所有子集组成的集合，而用 G^H 表示所有从 H 到 G 的函数形成的集合。下面是计算机安全系统 Bell-LaPadula 模型中的元素及含义：

1　$S=\{s_1,s_2,\cdots,s_n\}$--主体集 S：由所有 n 个主体 s_i 组成；

2　$O=\{o_1,o_2,\cdots,o_m\}$--客体集 O：由所有 m 个客体 o_i 组成；

3　$C=\{c_l\mid 1\leqslant l\leqslant q, c_1>c_2>\cdots>c_q\}$--密级集 C：由所有 q 个密级 c_l 组成；

4　$K=\{k_1,k_2,\cdots,k_p\}$…范畴集 K：由所有 p 个范畴级 k_i 组成；

5　$A=\{r,w,e,a,c\}$--访问属性集 A：由访问属性 read, write, execute, append 和 control 组成；

6　$RA=\{g,r,c,d\}$--请求元素集 RA：由 g(get, give),

*)本文的研究得到国家自然科学基金跨学科重点项目(No. 19931010)和国家973高科技项目基金(No. G1999035810、G1999035802)的资助。王贵林　博士，主要研究领域为协议分析和信息安全基础。卿斯汉　研究员，博士生导师，主要研究领域为信息安全理论和技术。倪惜珍　研究员，主要研究领域为信息安全技术。冯登国　研究员，博士生导师，主要研究领域为信息安全理论和技术。

r(release, rescind), c(change, create)和 d(delete)组成;

7 $R=S^+\times RA\times S^+\times O\times(A^+\cup F)$--请求集 R:由所有请求 r 组成;

8 $D=\{\underline{yes},\underline{no},\underline{error},\underline{?}\}$--决定集 D:由决定 $\underline{yes}$, $\underline{no}$, $\underline{error}$和$\underline{?}$组成;

9 $T=\{1,2,\cdots,t,\cdots\}$--指标集 T:由所有指标组成;

10 $F=\{f\mid f=(f_1,f_2,f_3,f_4)\}=C^S\times C^O\times P(K)^S\times P(K)^O$--密级-范畴向量集 F:由所有密级-范畴向量 $f=(f_1,f_2,f_3,f_4)$组成;

11 $MT=\{M_k\mid M_k=(m_{ij})_{n\times m}\}$--控制矩阵集 MT:由所有 $n\times m$ 阶的控制矩阵 M_k 组成, M_k 的元素 $m_{ij}\subseteq A$;

12 $V=\{v\mid v=(b,M,f)\}=P(S\times O\times A)\times M\times F$--状态集 V:由所有状态 $v=(b,M,f)$组成,其中 $b\subseteq S\times O\times A$, $M\in MT$, $f\in F$;

13 $X=R^T=\{x\mid x=x_1x_2\cdots x_t\cdots\}$--请求序列集 X:由所有请求序列 x 组成;

14 $Y=D^T=\{y\mid y=y_1y_2\cdots y_t\cdots\}$--决定序列集 Y:由所有决定序列 y 组成;

15 $Z=V^T=\{z\mid z=z_1z_2\cdots z_t\cdots\}$--状态序列集 Z:由所有状态序列 z 组成;

16 $W\subseteq R\times D\times V\times V$--状态转移关系 W;

17 $\sum(R,D,W,z_0)\subseteq X\times Y\times Z$--系统 $\sum(R,D,W,z_0)$:由状态转移关系 W 及初始状态 z_0决定。

现在对上面的密级-范畴向量集 F 作一点解释。作为 F 的元素,每个密级-范畴向量 $f(f_1,f_2,f_3,f_4)$由四个分量函数组成:

(1)主体密级函数 $f_1:S\to C$: $f_1(s)$表示主体 s 的密级, $f_1(s)$越大, s 的访问密级越高;

(2)客体密级函数 $f_2:O\to C$: $f_2(o)$表示客体 o 的密级, $f_2(o)$越大, o 越不易被访问;

(3)主体范畴函数 $f_3:S\to P(K)$: $f_3(s)$表示主体 s 可以涉及的范畴, $f_3(s)$越大, s 可涉及的范围越广;

(4)客体范畴函数 $f_4:O\to P(K)$: $f_4(o)$表示客体 o 涉及的范畴, $f_4(o)$越大,访问 o 的需知范围越广;

所以,对安全性的直观要求就是:主体访问客体时,要求主体的密级和范畴比客体的密级和范畴大。严格的安全性概念见定义4至定义8。

利用上述的符号,现在来给出 Bell-LaPadula 模型中的一系列定义。

定义1 由状态转移关系 W 及初始状态 z_0决定的系统 $\sum(R,D,W,z_0)$是指集合:

$$\sum(R,D,W,z_0)=\{(x,y,z)\in X\times Y\times Z\mid \forall t\in T,(x_t,y_t,z_t,z_{t-1})\in W\}.$$

一般来讲,定义1中的初始状态 $z_0=(\phi,M,f)$。

定义2 系统 $\sum(R,D,W,z_0)$中的每个元素 (x,y,z)称为系统的一个表演(appearance)。

定义3 $R\times D\times V\times V$ 中的元素 (r_t,d_t,v^*,v)称为系统 $\sum(R,D,W,z_0)$的一个动作(action)⇔存在系统 $\sum(R,D,W,z_0)$中的某个表演 (x,y,z)和某个指标 $t\in T$ 使得

$$(r_t,d_t,v^*,v)=(x_t,y_t,z_t,z_{t-1})$$

换句话说,所有在系统的某个表演中出现的四元组 (r_t,d_t,v^*,v)都叫系统的一个动作。动作 (r_t,d_t,v^*,v)的含义在于,在状态 v 下输入请求 r_t,系统就输出决定 d_t,并将状态切换到 v^*。从上面的三个定义知,多个动作构成表演,而多个表演构成系统。

另外,根据系统的定义,容易知道:若 (r_t,d_t,v^*,v)是系统 $\sum(R,D,W,z_0)$的一个动作,则 $(r_t,d_t,v^*,v)\in W$。

定义4 称 $(s,o,\underline{x})\in S\times O\times A$ 满足相对于 f 的安全性条件⇔下面的两个条件成立一个:(1) $\underline{x}=\underline{e}$ or $\underline{x}=\underline{a}$ or $\underline{x}=\underline{c}$;(2)($\underline{x}=\underline{r}$ or $\underline{x}=\underline{w}$) and ($f_1(s)\geqslant f_2(o)$ and $f_3(s)\supseteq f_4(o)$)。

此时,简记作 (s,o,x)满足 $sc|f$。

定义5 状态 $v=(b,M,f)$称为安全状态⇔所有的 $(s,o,x)\in b$ 都满足 $sc|f$。

定义6 状态序列 $z=z_1z_2\cdots z_t\cdots$称为安全状态序列⇔任意 $t\in T$, z_t 是安全状态。

定义7 系统 $\sum(R,D,W,z_0)$中的某个表演 (x,y,z)称为安全表演⇔z 是安全状态序列。

定义8 系统 $\sum(R,D,W,z_0)$称为安全系统⇔初始状态 z_0是安全的,且每个表演 $(x,y,z)\in\sum(R,D,W,z_0)$都是安全表演。

定义9 给定主体 $s\in S$、主客体访问关系 $b\subseteq S\times O\times A$ 和访问属性子集 $B\subseteq A$,记 $b(s;B)$为:

$$b(s;B)=\{o\in O\mid \exists\ \underline{x}\in B,s.t.,(s,o,\underline{x})\in b\}$$

称 $b(s;B)$为在主客体访问关系 b 和访问属性子集 B 下,与主体 s 相联系的客体集。

有时,我们也将 $b(s;B)$中 B 的元素简单地罗列出来,用逗号分开,而不写大括号。比如有

$b(s;\{\underline{r},\underline{w}\})=b(s;\underline{r},\underline{w})$和 $b(s;\{\underline{a}\})=b(s;\underline{a})$。

定义10 一个状态 $v=(b,M,f)$称为满足 $*$-性质⇔对任意的 $s\in S$,下面的条件成立:若 $b(s;\underline{w},\underline{a})\neq\phi$ 和 $b(s;\underline{w},\underline{r})\neq\phi$,则对$\forall\ o_1\in b(s;\underline{w},\underline{a})$和$\forall\ o_2\in b(s;\underline{w},\underline{r})$,都满足:

$$f_2(o_1)\geqslant f_2(o_2)\text{且 }f_4(o_1)\supseteq f_4(o_2)$$

有了状态满足 * -性质的概念，可类似于安全性的概念一样，定义状态序列、系统行为和系统满足 * -性质的概念。

规则 ρ 就是一个函数 $\rho: R\times V\to D\times V$。规则是状态转移关系的特例，因为给定一个规则 ρ 也就决定了一个状态转移关系 $W(\rho)=\{(r_k,d_l,v^*,v)\mid \rho(r_k,v)=(d_l,v^*)\}$。

定义11 设 ρ 是规则，我们有以下的定义：

(1)ρ 称为保持安全性的规则当且仅当对任意的 $(r_k,v)\in R\times V$，若 $\rho(r_k,v)=(d_l,v^*)$ 且状态 v 是安全的，则状态 v^* 也是安全的。

(2)ρ 称为保持 * -性质的规则当且仅当对任意的 $(r_k,v)\in R\times V$，若 $\rho(r_k,v)=(d_l,v^*)$ 且状态 v 满足 * -性质，则状态 v^* 也满足 * -性质。

三、安全计算机系统 Bell-LaPadula 模型的主要结论

文[11]中给出了如下所述的定理0。如果定理0是正确的，那么它就提供了信息系统安全的充分必要条件。可惜的是，定理0是错误的。下面，先叙述错误的定理0，然后再给出与定理0相似但结论正确的定理1和与定理1等价的定理2。最后，我们再证明其它几个主要的定理。

定理0[11] 系统 $\sum(R,D,W,z_0)$ 对于任何安全的初始状态 z_0 来说是安全的，当且仅当对于所有的 $(r_j,d_j,(b^*,M^*,f^*),(b,M,f))\in W$，下面的条件(1)和(2)都成立

(1)任意 $(s,o,\underline{x})\in b^*-b$ 满足 $sc\mid f^*$；

(2)每一个不满足 $sc\mid f^*$ 的 $(s,o,\underline{x})\in b$ 不属于 b^*。

定理0给出的条件(1)和(2)，实际上是系统安全的一个充分条件，但不是必要条件。所以定理的结论是错误的。错误的原因在于，系统安全时 W 中每个元素不一定满足条件(1)和(2)，但系统的每个动作却一定满足条件(1)和(2)。也就是说，下面的定理1成立。

定理1 系统 $\sum(R,D,W,z_0)$ 对于任何安全初始状态 z_0 来说是安全的，当且仅当 W 中的所有动作 $(r_j,d_j,(b^*,M^*,f^*),(b,M,f))$ 使下面的条件(1)和(2)都成立：

(1)任意 $(s,o,\underline{x})\in b^*-b$ 满足 $sc\mid f^*$；

(2)每一个不满足 $sc\mid f^*$ 的 $(s,o,\underline{x})\in b$ 不属于 b^*。

证明：条件(2)等价于它的逆否命题：属于 b^* 的、b 的元素 $(s,o,\underline{x})$ 一定满足 $sc\mid f^*$，即：

$\forall(s,o,\underline{x})\in b^*\cap b\Rightarrow(s,o,\underline{x})$ 满足 $sc\mid f^*$

这样，把条件(1)和条件(2)合并，我们就得出 $\forall(s,o,\underline{x})\in(b^*-b)\cup(b^*\cap b)\Rightarrow(s,o,\underline{x})$ 满足 $sc\mid f^*$，此即

$\forall(s,o,\underline{x})\in b^*\Rightarrow(s,o,\underline{x})$ 满足 $sc\mid f^*$

这也就是说，条件(1)和条件(2)与下面的条件等价：

状态 $v^*=(b^*,M^*,f^*)$ 是安全的。

所以，要证明本定理，只需要证明命题：系统 $\sum(R,D,W,z_0)$ 对于任何安全的初始状态 z_0 来说是安全的⇔对于所有动作 $(r_j,d_j,v^*,v)\in W$ 来说 v^* 是安全的。

而根据定义6、7、8，容易知道该命题正确。所以定理1证毕。

由定理1的证明，我们实际上已经得到了与定理1等价的下述定理2。

定理2 系统 $\sum(R,D,W,z_0)$ 是安全的⇔初始状态 z_0 是安全的且对于 $\sum(R,D,W,z_0)$ 中的每个动作 $(r_j,d_j,v^*,v)\in W$ 来说，状态 v^* 是安全的。

定理3 如果初始状态 z_0 是安全的，且状态转移关系 W 满足：系统 $\sum(R,D,W,z_0)$ 中的每个动作 $(r_j,d_j,(b^*,M^*,f^*),(b,M,f))\in W$ 都使下面两个条件成立：(1)$f^*=f$；(2)任意 $(s,o,\underline{x})\in b^*-b$ 满足 $sc\mid f^*$，那么 $\sum(R,D,W,z_0)$ 是安全系统。

证明：可用反证法，细节省略。

定义12 给定相对于 R,D 和 V 的规则集 $\omega=\{\rho_1,\rho_2,\cdots,\rho_s\}$，定义集合 $W(\omega)$ 如下：

(1)$(r_k,\underline{?},v,v)\in W(\omega)\Leftrightarrow\forall i(1\leqslant i\leqslant s),\rho(r_k,v)=(\underline{?},v)$；

(2)$(r_k,\underline{error},v,v)\in W(\omega)\Leftrightarrow\exists i,j(1\leqslant i\leqslant j\leqslant s)$.$t(\rho_i(r_k,v)\neq(\underline{?},v^*)$ and $\rho(r_k,v)\neq(\underline{?},v^*))$；

(3)$(r_k,d_l,v^*,v)\in W(\omega)\Leftrightarrow\exists i(1\leqslant i\leqslant s),\rho(r_k,v)=(d_l,v^*)\neq(\underline{?},v^*)$，

$W(\omega)$ 称为由规则集 ω 按自然方式合成的状态转移关系(简称为 ω 的自然合成)，

$W(\omega)$ 的含义是这样的：(1)若每个规则 ρ_i 都不处理 (r_k,v)，则 $W(\omega)$ 也不处理 (r_k,v)；(2)若至少有两个 ρ_i,ρ_j 对 (r_k,v) 有不同的处理，则 $W(\omega)$ 指出 (r_k,v) 是一个错误请求；(3)若只有唯一的一个 ρ_i 处理 (r_k,v)，则 $W(\omega)$ 对 (r_k,v) 的处理就是 ρ_i 对 (r_k,v) 的处理。

定理4 若 ω 是一个保持安全性的规则集，z_0 是安全的初始状态，则 $\sum(R,D,W(\omega),z_0)$ 是一个安全系统。

定理5 若 ω 是一个保持 * -性质的规则集，z_0 是一个满足 * -性质的初始状态，则系统 $\sum(R,D,W(\omega),z_0)$ 是一个满足 * -性质的系统。

定理4和定理5的证明并不难，在此略去不证。

定理6 状态 $v=(b,M,f)$ 是安全的且 $(s,o,\underline{x})\notin b$，令 $b^*=b\cup\{(s,o,\underline{x})\}$，$v^*=(b^*,M,f)$。于是有：

(1)若 $\underline{x}=\underline{e}$ 或 $\underline{x}=\underline{a}$ 或 $\underline{x}=\underline{c}$，则 v^* 是安全的；

(2)若 $\underline{x}=\underline{r}$ 或 $\underline{x}=\underline{w}$，则 v^* 是安全的 $\Leftrightarrow f_1(s)\geqslant f_2(o)$ 且 $f_2(s)\supseteq f_4(o)$。

证明：由 $(s,o,\underline{x})$ 满足 $sc|f$ 的定义5和状态安全的定义6，本定理即可成立。

定理7 假设状态 $v=(b,M,f)$ 满足 *-性质且 $(s,o,\underline{x})\notin b$，而令 $b^*=b\cup\{(s,o,\underline{x})\}$，$v^*=(b^*,M,f)$，于是有：

(1)若 $\underline{x}=\underline{e}$ 或 $\underline{x}=\underline{c}$，则 v^* 满足 *-性质；

(2)若 $\underline{x}=\underline{a}$，则 v^* 满足 *-性质 $\Leftrightarrow f_2(o)\geqslant f_2(o')$ and $f_4(o)\supseteq f_4(o')$，$\forall\ o'\in b(s:\underline{r},\underline{w})$；

(3)若 $\underline{x}=\underline{r}$，则 v^* 满足 *-性质 $\Leftrightarrow f_2(o)\leqslant f_2(o')$ and $f_4(o)\subseteq f_4(o')$，$\forall\ o'\in b(s:\underline{a},\underline{w})$；

(4)若 $\underline{x}=\underline{w}$，则 v^* 满足 *-性质 $\Leftrightarrow$ 下面三个条件都成立：(a) $f_2(o)\geqslant f_2(o')$ and $f_4(o)\supseteq f_4(o')$，$\forall\ o'\in b(s:\underline{r})$；(b) $f_2(o)\leqslant f_2(o')$ and $f_4(o)\subseteq f_4(o')$，$\forall\ o'\in b(s:\underline{a})$；(c) $f_2(o)=f_2(o')$ and $f_4(o)=f_4(o')$，$\forall\ o'\in b(s:\underline{w})$。

证明：在此仅证明情形(3)，其他类似。

(3)$\Rightarrow$：由 $\underline{x}=\underline{r}$ 知 $b^*=b\cup\{(s,o,\underline{r})\}$，于是 $o\in b^*(s:\underline{r},\underline{w})$；而 v^* 满足 *-性质，所以根据定义10，我们有：$f_2(o)\leqslant f_2(o')$ and $f_4(o)\subseteq f_4(o')$，$\forall\ o'\in b(s:\underline{a},\underline{w})$。

(3)$\Leftarrow$：根据定义10，要证明 v^* 满足 *-性质，只需要证明：

$$\forall\ (o',o_2)\in b^*(s:\underline{a},\underline{w})\times b^*(s:\underline{r},\underline{w})\Rightarrow f_2(o_2)\leqslant f_2(o') \text{ and } f_4(o_2)\subseteq f_4(o'). \quad (1)$$

由 $\underline{x}=\underline{r}$ 知 $b^*=b\cup\{(s,o,\underline{r})\}$，故 $b^*(s:\underline{a},\underline{w})=b(s:\underline{a},\underline{w})$，$b^*(s:\underline{r},\underline{w})=b(s:\underline{r},\underline{w})\cup\{o\}$。所以，要证明(1)式等价于证明下式：

$$\forall\ (o',o_2)\in b(s:\underline{a},\underline{w})\times(b(s:\underline{r},\underline{w})\cup\{o\})\Rightarrow f_2(o_2)\leqslant f_2(o') \text{ and } f_4(o_2)\subseteq f_4(o'). \quad (2)$$

若 $o_2=o$，则根据假设，(2)式的右端已经成立。若 $o_2\in b(s:\underline{r},\underline{w})$，则根据 $v=(b,M,f)$ 满足 *-性质，所以(2)式的右端也成立。证毕。

上述四个定理的意义在于：按照需要，我们可以运用定理6和定理7构造出一个个保持安全性或 *-性质的规则。对这些保持安全性或 *-性质的规则进行自然合成，根据定理4和定理5，我们就得到了一个安全的或满足 *-性质的系统。

结束语 本文在较为详细地介绍了安全计算机系统的 Bell-LaPadula 形式化模型之后，对其中的主要结果给出了证明，并指出了几个主要定理的现时意义。为便于理解和使用 Bell-LaPadula 模型，我们引进了一些新的概念，比如规则的合成等。同时，本文还指出文[11]中给出的安全信息系统的充分必要条件是错误的。利用动作的概念，我们给出了正确的充分必要条件。我们今后的目标是研究由文[12]给出的改进 BLP 模型的形式化证明。

参 考 文 献

1 Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations: [MITRE Technical Report 2547]. Volume I. National Technical Information Service, 1973. http: // www. mitre org/resources/centers/infosec/secure_computers/

2 LaPadula L J, Bell D E. Secure Computer Systems. A Mathematical Model: [MITRE Technical Report 2547]. Volume I. National Technical Information Service, 1973. http: // www mitre. org/resources/centers/infosec/secure_computers/

3 Bell D E, LaPadula L J. Secure Computer Systems: Unified Exposition and Multics Interpretation: [Technical Report ESD-TR-75-306] The Mitre Corporation, Bedford MA. USA, March 1976

4 Landwehr C E. Best Available Technologies for Computer Security. IEEE Computer Society, July, 1983

5 McLean J. A Comment on the 'Basic Security Theorem' of Bell and LaPadula. Information Processing Letters, 1985, 20(2): 67～70

6 Sutherland I. Relating Bell-LaPadula-Style Security Models to Information Models. In: Proc. of the Computer Security Foundations Workshop, Franconia, NH. 1988

7 Abrams M, LaPadula L J, Eggers K, Olson I. A Generalized Framework for Access Control, an Informal Description. In: Proc. of the 13th National Computer Security Conf. 1990. 134～143

8 Verschuren J, Govaerts R, Vandewalle R. Realization of the Bell-LaPadula Security Policyin an OSI Distributed System Using Asymmetric and Symmetric Cryptographic Algorithms. In: Proc. of the Computer Security Foundations Workshop V IEEE Computer Society Press, 1992. 168～178

9 LaPadula L J. Foreword for Republishing of the Bell-LaPadula Model. Journal of Computer Security, 1996, 4: 233～238

10 Focardi R, Martinelli F. A Uniform Approach for the Definition of Security Properties. In: Proc. of World Congress on Formal Methods. FM'99), Springer, LNCS 1708, 1999. 794～813

11 徐志太，南湘浩. 信息保密 Bell-LaPadula 模型的形式化描述与证明. 信息和通信安全——CCICS'99. 中国第一届信息和通信安全学术会议论文集. 科学出版社，2000

12 刘文清，刘海峰，卿斯汉. 一个修改 BLP 安全模型的设计及在 SecLinux 的应用. 软件学报(已录用，待发表)，2000年11月