一种具有可信度特征的多级安全模型

谭智勇, 刘 铎, 司天歌, 戴一奇
(清华大学计算机科学与技术系, 北京 100084)

摘 要: 为解决现有多级安全系统中存在的可信主体安全隐患和系统可用性较差的问题, 本文提出一种具有可信度特征的多级安全模型. 通过在 BLP 模型中增加主客体的可信度标记和可信度评估函数, 该模型可以准确地评估访问请求的可信度以及主客体可信度随访问行为变化的情况. 以此可信度评估机制为基础, 该模型建立了对可信主体的约束机制, 使系统可以赋予更多主体有限程度的特权, 增加了系统的灵活性和可用性.

关键词: 多级安全; 可信度; BLP (Bell-La Padula) 安全模型; 访问控制
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2008) 08-1637-05

A Multilevel Security Model with Credibility Characteristics

TAN Zhi-yong, LIU Duo, SI Tian-ge, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*)

Abstract: A multilevel security (MLS) model with credibility characteristics was proposed to solve the problem of trusted subjects' hidden security flaw and poor system usability in present MLS systems. By introducing credibility labels of subjects and objects and credibility evaluation functions in original BLP model, it can evaluate credibility of access requests as well as corresponding credibility variation of subjects and objects. Since this model establishes restriction mechanism against trusted subjects and assigns limited privileges to all subjects, it is more flexible and practicable than present security-label based MLS models.

Key words: multilevel security; credibility; BLP security model; access control

1 引言

BLP 模型是实现多级安全(Multilevel Security, MLS)的经典安全模型, 该模型强制要求所有非可信主体对客体的访问均满足三个基本安全属性: ss-属性, * -属性和 ds-属性[1~3]. 模型同时定义允许违反* -属性但不会由此破坏系统安全性的主体为可信主体[1], 通过可信主体的违规操作保证实际系统的正常运行. 但这种处理方式存在两个问题: 首先, 系统缺乏针对可信主体的约束机制, 使其能随意进行违反* -属性的违规操作; 其次, 约束机制的缺失致使系统必须严格控制可信主体的数量, 导致系统中绝大部分主体是访问行为严格受限的非可信主体, 系统的可用性很差.

针对可信主体的约束机制问题, 研究者设计出多种基于 BLP 模型的改进模型和实施策略. Bell 所提 BLP 扩展模型中, 每个主体对应一个($\lambda_{max}(s_i)$, $\lambda_{min}(s_i)$) 二元组, 主体对安全标记处于此二元组之间客体的访问不必遵守 BLP 的基本安全属性[4]. 其它研究人员提出了部分可信主体及相关概念[5,6], 在一定程度上实现了对可信主体行为的约束和限制. 但这些约束机制在本质上是静态的, 被授予的特权等级无法随可信主体执行特权操作的情况进行动态调整.

针对提高系统可用性的问题, 研究者也提出了一些改进方案. Bell 的 BLP 扩展模型的核心即是允许主体在受控的范围内违反 ss-属性和* -属性, 从而提高系统的可用性[4]. 石文昌等提出的 ABLP 模型[7] 和季庆光等提出的 DBLP 模型[6] 能动态改变主体的当前安全标记或安全标记范围, 以此提高了 BLP 模型的灵活性. 但这些改进方案在系统的实际运行中, 安全标记的动态调节区域会随着违规访问的进行而迅速缩小, 安全标记动态调整机制也随之失效, 因此并未从根本上解决系统可用性的问题.

2 一种具有可信度特征的多级安全模型(CBLP)

为解决上述问题, 本文提出访问行为和主客体具有可信度特征的 CBLP(Credibility-based BLP) 多级安全访问控制模型. 新模型以可信度作为判据实现对主体的有限信任, 允许主体在指定的可信度阈值范围内进行违规操作. 下面将借鉴文献[8] 的模型表达方式, 对 CBLP 模型进行详细的描述.

收稿日期: 2007-07-09; 修回日期: 2008-04-28
基金项目: 国家自然科学基金(No. 60673065)

2.1 CBLP 模型状态变量和系统的定义

本节将给出在 CBLP 模型中使用的主要的状态变量.

(1) 主体集合 S: $\mathscr{P}$SUBJECT, 它由可信主体集合 S_t 和非可信主体集合 S_{ut} 两部分组成.

客体集合 O: $\mathscr{P}$OBJECT.

安全标记集合 L: $\mathscr{P}$LEVEL, 安全标记 LEVEL 是安全等级和安全范畴的二元组.

可信度集合 CR: $\mathscr{P}$CREDIBILITY.

访问模式集合 A: $\mathscr{P}$OPERATION.

时序集合 T: $\mathscr{P}$TIME.

(2) 安全标记的控制关系 $\geqslant$: LEVEL $\times$ LEVEL.

访问许可函数 M: $O \rightarrow S \times A$, 访问方式集合 A 可能的操作有:

$\underline{r}$- 一个主体能以只读(read)的方式访问一个客体;

$\underline{a}$- 一个主体能以只写(append)的方式访问一个客体;

$\underline{w}$- 一个主体能以读写(write)的方式访问一个客体.

(3) 当前访问集合 $B \subseteq \mathscr{P}(S \times O \times A)$, 表明被当前系统允许的访问操作.

(4) 安全标记函数集合 F,

$$F = \{(f_s, f_o, f_c) \mid \forall s \in S, f_s(s) \geqslant f_C(s)\}$$

其中: (a) f_s: $S \rightarrow L$, 为主体最大安全标记函数;

(b) f_o: $O \rightarrow L$, 为客体安全标记函数;

(c) f_c: $S \rightarrow L$, 为主体当前安全标记函数.

(5) 可信度函数集合 G,

$$G = \{(g_s, g_o, g_s^M, g_o^M) \mid \forall s \in S, \forall o \in O, (g_s(s) \leqslant g_s^M(s)) \wedge (g_o(o) \leqslant g_o^M(o))\}$$

其中: (a) g_s: $S \rightarrow CR$, 为主体当前可信度函数;

(b) g_o: $O \rightarrow CR$, 为客体当前可信度函数;

(c) g_s^M: $S \rightarrow CR$, 为主体可信度阈值函数;

(d) g_o^M: $O \rightarrow CR$, 为客体可信度阈值函数.

(6) 可信度评估函数集合 CV, $CV = \{(cv_r, cv_s, cv_o)\}$, 其中 (cv_r, cv_s, cv_o): $CR \times CR \times A \times L \times L \rightarrow CR \times CR \times CR$, 它们分别为访问请求可信度评估函数、主体可信度评估函数和客体可信度评估函数. 该函数集合的详细描述请参见 2.3.1 节. 此外, 定义常数 g_r^M 为系统违规请求的可信度阈值.

(7) 层次关系集合 H, 表明当前客体间的层次(包含)关系.

(8) 请求集合 R, 表明系统请求的各种操作.

(9) 判断集合 D, $D = \{\underline{yes}, \underline{no}, \underline{error}, \underline{?}\}$, 表明对系统请求的回复.

基于上述状态变量, 以下给出 CBLP 模型中系统的定义:

定义 1 系统 $\sum(R, D, W, z_0)$ 定义为:

$$\sum(R, D, W, z_0) = \{(x, y, z) \mid x \in R^{\mathrm{T}} \wedge y \in D^{\mathrm{T}} \wedge z \in V^{\mathrm{T}} \wedge (\forall t \in T, (x_t, y_t, z_t, z_{t-1}) \in W)\}$$

其中 $V \subseteq B \times M \times F \times G \times CV \times H$ 是系统状态的集合, 表明系统所处的状态; $W \subseteq R \times D \times V \times V$ 是状态转换关系的集合, 表明在指定状态下, 请求所产生的下一状态及判定; z_0 是系统初始状态.

与 BLP 模型相比, CBLP 模型的最大变化在于变量类型中增加了可信度标记, 并在状态变量中相应地增加了可信度函数和可信度评估函数. 这种可信度在数学上能用 Lukasiewicz 无穷值逻辑系统的逻辑真值来表达, 即用 [0, 1] 区间的实数 r 表示主客体和访问行为的可信度以及主客体的可信度阈值. 这样可信主体和非可信主体的定义可由可信度阈值统一表达: 可信主体为可信度阈值小于 1 的主体, 非可信主体为可信度阈值等于 1 的主体.

2.2 CBLP 模型状态迁移规则

CBLP 模型中共有四条状态迁移规则: 规则 1 描述了当前访问请求不违反 ss-特性和 * -特性时的系统状态迁移过程; 规则 2、规则 3 和规则 4 分别描述了当前访问请求分别为 $\underline{r}$、$\underline{a}$ 和 $\underline{w}$, 满足 ss-特性但违反 * -特性时的系统状态迁移过程.

规则 1 在 (b, M, f, g, cv, H) 状态, $x \in M_{ij} \in M$, $rq(s_i, o_j, x)$ 不破坏 BLP 模型所述的 ss-特性和 * -特性时, 对 $rq(s_i, o_j, x)$ 的处理 ($x = \underline{r}$, $\underline{a}$ 或 $\underline{w}$):

(1) 对 $rq(s_i, o_j, x)$ 授权, 构造 b^*, 使得 $b^* = \{(s_i, o_j, x)\} \cup b$;

(2) 系统进入 V^* 状态, $V^* = (b^*, M, f, g, cv, H)$.

规则 2 在 (b, M, f, g, cv, H) 状态, $\underline{r} \in M_{ij} \in M$, $f_s(s_i) \geqslant f_o(o_j) \wedge f_c(s_i) ! \geqslant f_o(o_j)$ 时, 对 $rq(s_i, o_j, \underline{r})$ 的处理:

(1) $(g_r(rq), g_s^*(s_i), g_o^*(o_j)) = cv(g_s(s_i), g_o(o_j), \underline{r}, f_c(s_i), f_o(o_j))$;

(2) If $(g_r(rq) \geqslant g_r^M)$ and $(g_s^*(s_i) \geqslant g_s^M(s_i))$ and $(g_o^*(o_j) \geqslant g_o^M(o_j))$, then

(a) 构造 g^*, 使得 $g^* = (g_s^*(s_i), g_o^*(o_j), g_s^M(s_i), g_o^M(o_j))$;

(b) 对 $rq(s_i, o_j, \underline{r})$ 授权, 构造 b^*, 使得 $b^* = \{(s_i, o_j, \underline{r})\} \cup b$;

(c) 系统进入 V^* 状态, $V^* = (b^*, M, f, g^*, cv, H)$.

else 拒绝 $rq(s_i, o_j, \underline{r})$.

规则 3 在 (b, M, f, g, cv, H) 状态, $\underline{a} \in M_{ij} \in M$, $f_o(o_j) ! \geqslant f_c(s_i)$ 时, 对 $rq(s_i, o_j, \underline{a})$ 的处理:

(1) $(g_r(rq), g_s^*(s_i), g_o^*(o_j)) = cv(g_s(s_i), g_o(o_j), \underline{a}, f_c(s_i), f_o(o_j))$;

(2) If $(g_r(rq) \geqslant g_r^M)$ and $(g_s^*(s_i) \geqslant g_s^M(s_i))$ and $(g_o^*(o_j) \geqslant g_o^M(o_j))$, then

(a) 构造 g^*, 使得 $g^* = (g_s^*(s_i), g_o^*(o_j), g_s^M(s_i), g_o^M(o_j))$;

(b) 对 $rq(s_i, o_j, \underline{a})$ 授权, 构造 b^*, 使得 $b^* = \{(s_i, o_j, \underline{a})\} \cup b$;

(c) 系统进入 V^* 状态, $V^* = (b^*, M, f, g^*, cv, H)$.

else 拒绝 $rq(s_i, o_j, \underline{a})$.

规则 **4**　在 (b, M, f, g, cv, H) 状态, $\underline{w} \in M_{ij} \in M$, $f_s(s_i) \geqslant f_o(o_j) \wedge (f_c(s_i) ! \geqslant f_o(o_j) \vee f_o(o_j) ! \geqslant f_c(s_i))$ 时, 对 $rq(s_i, o_j, \underline{w})$ 的处理:

(1) $(g_r(rq), g_s^*(s_i), g_o^*(o_j)) = cv(g_s(s_i), g_o(o_j), \underline{w}, f_c(s_i), f_o(o_j))$;

(2) If $(g_r(rq) \geqslant g_r^M)$ and $(g_s^*(s_i) \geqslant g_s^M(s_i))$ and $(g_o^*(o_j) \geqslant g_o^M(o_j))$, then

(a) 构造 g^*, 使得 $g^* = (g_s^*(s_i), g_o^*(o_j), g_s^M(s_i), g_o^M(o_j))$;

(b) 对 $rq(s_i, o_j, \underline{w})$ 授权, 构造 b^*, 使得 $b^* = \{(s_i, o_j, \underline{w})\} \cup b$;

(c) 系统进入 V^* 状态, $V^* = (b^*, M, f, g^*, cv, H)$.

else 拒绝 $rq(s_i, o_j, \underline{w})$.

2.3　CBLP 模型可信度评估函数的设计

2.3.1　设计原则与边界条件

可信度评估函数 (cv_r, cv_s, cv_o) 决定了访问请求的可信程度以及主客体的可信度随访问行为的改变情况, 其定义如下:

定义 **2**　可信度评估函数 (cv_r, cv_s, cv_o) 定义为:

$(cv_r, cv_s, cv_o): CR \times CR \times A \times L \times L \rightarrow CR \times CR \times CR$

$(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) \mapsto (g_r(rq), g_s^*(s_i), g_o^*(o_j))$

其自变量和因变量的符号和定义如下: 对于访问请求 $rq(s_i, o_j, x)$, 自变量 $g_s(s_i)$ 为主体可信度、$g_o(o_j)$ 为客体可信度、x 为请求类型、$f_c(s_i)$ 为主体当前安全级别、$f_o(o_j)$ 为客体安全级别; 因变量 $g_r(rq)$ 为该请求的可信度、$g_s^*(s_i)$ 为请求成功后主体的新可信度、$g_o^*(o_j)$ 为请求成功后客体的新可信度.

可信度评估函数的设计遵循如下原则:

(1) $g_r(rq)$、$g_s^*(s_i)$ 和 $g_o^*(o_j)$ 的取值均为 0 和 1 之间的实数;

(2) s_i 和 o_j 的可信度越低, $g_r(rq)$ 的可信度越低, 反之亦然;

(3) 客体安全级别 $f_o(o_j)$ 越高, $g_r(rq)$ 的可信度越低, 反之亦然;

(4) 在违反 * - 属性的情况下, $f_c(s_i)$ 和 $f_o(o_j)$ 之间相差的程度越大, 表明违规的程度越大, $g_r(rq)$ 的可信度越低, 反之亦然.

同时, 该可信度评估函数应满足如下的边界条件:

(1) 可信度为 0 的主体对可信度为 0 的客体的访问应被视为绝对不可信, 即: $g_s(s_i) = g_o(o_j) = 0$ 时, $g_r(rq) = g_s^*(s_i) = g_o^*(o_j) = 0$;

(2) 可信度为 1 的主体对可信度为 1 的客体进行非违规访问应被视为绝对可信, 即: $g_s(s_i) = g_o(o_j) = 1$, 且满足 $f_c(s_i) \geqslant f_o(o_j)\ (x = \underline{r}), f_o(o_j) \geqslant f_c(s_i)\ (x = \underline{a})$ 或 $f_s(s_i) \geqslant f_o(o_j) \wedge f_c(s_i) = f_o(o_j)\ (x = \underline{w})$ 时, $g_r(rq) = g_s^*(s_i) = g_o^*(o_j) = 1$.

2.3.2　可信度评估函数的设计示例

基于以上的设计原则和边界条件, 可以进行可信度评估函数的设计. 由于该函数的具体形式应该由多级安全系统的设计者来选择, 所以本节仅列举一些示例来说明该函数的一般设计思路.

可信度评估函数有多种表达方式, 其中较简单的可采用如下的线性递减形式:

$$g_r(rq) = cv_r(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = \max\left(\frac{g_s(s_i) + g_o(o_j)}{2} - \Delta f_x(s_i, o_j) \cdot \sigma_0, 0\right) \quad (1)$$

$$g_s^*(s_i) = cv_s(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = \max\left(g_s(s_i) - \Delta f_x(s_i, o_j) \cdot \sigma_0, 0\right) \quad (2)$$

$$g_o^*(o_j) = cv_o(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = \max\left(g_o(o_j) - \Delta f_x(s_i, o_j) \cdot \sigma_0, 0\right) \quad (3)$$

其中 σ_0 表示主客体对应一个违规等级的可信度下降幅度; $\Delta f_x(s_i, o_j)$ 为违规等级评估函数, 表示主体 s_i 对客体 o_j 进行 x 操作的违规等级. 在不考虑主客体范畴因素的前提下, 安全标记可简化为主客体的安全等级. 这样违规等级评估函数具有如下的计算公式:

$$\Delta f_x(s_i, o_j) = \begin{cases} \max\left((f_o(o_j) - f_c(s_i)), 0\right), & x = \underline{r} \\ \max\left((f_c(s_i) - f_o(o_j)), 0\right), & x = \underline{a} \\ \mathrm{abs}\left(f_c(s_i) - f_o(o_j)\right), & x = \underline{w} \end{cases} \quad (4)$$

线性递减形式的评估函数虽然形式简单, 但较难引入对高安全标记客体违规操作的额外惩罚机制, 也很难把主客体在违规操作中可信度的惩罚值与其当前可信度联系起来. 为解决这些问题, 可采用负指数形式的评估函数, 如以当前访问行为中相关主客体可信度的算术平均作为基础, 并乘以一个表示其它影响因素的负指数因子来评估主客体可信度随着访问行为而变化的过程. 函数表达式可采用如下形式:

$$g_r(rq) = cv_r(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = \frac{g_s(s_i)+g_o(o_j)}{2} \cdot e^{-k \cdot \frac{f_o(o_j)}{f_o^M} \cdot \frac{\Delta f_x(s_i,o_j)}{f_c(s_i)}} \quad (5)$$

$$g_s^*(s_i) = cv_s(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = g_s(s_i) \cdot g_r(rq) \quad (6)$$

$$g_o^*(o_j) = cv_o(g_s(s_i), g_o(o_j), x, f_c(s_i), f_o(o_j)) = g_o(o_j) \cdot g_r(rq) \quad (7)$$

其中式(5)中 $\Delta f_x(s_i, o_j)$ 函数的意义与线性递减形式的评估函数中的相同,f_o^M 为系统客体最大安全级别, k 表示影响访问行为可信度的其它因素,其值的选取与访问行为的类型有关, 也与主客体的可信度随违规访问的衰减速度相关.

2.4 CBLP 系统应用示例

下面将用一个系统示例说明 CBLP 的应用. 假设系统中存在一个主体 s_1 和三个客体 o_1、o_2 和 o_3, 忽略主客体的范畴因素, 主客体的可信度阈值和系统初始参考值如表 1 所示:

表 1 系统中各主客体的可信度阈值和系统初始参考值

	s_1	o_1	o_2	o_3
f_o	—	1	2	3
f_s	2	—	—	—
f_c	2	—	—	—
g_o^M/g_s^M	0.80	0.60	0.70	0.80
g_o/g_s 初始值	1.00	1.00	1.00	1.00

下面的计算过程将采用 2.3.2 节中负指数形式的可信度评估函数, 即式(4)~(7). 对式(5)中的 k 取值如下: 当 $x=\underline{r}$ 或 $\underline{a}$ 时, $k=0.3$; 当 $x=\underline{w}$ 时, $k=0.4$. 并设定系统的 g_r^M 值为 0.80. 假设 s_1 依次对客体发出以下的数据请求: $rq_1(s_1, o_2, \underline{r})$, $rq_2(s_1, o_1, \underline{w})$, $rq_3(s_1, o_3, \underline{r})$, $rq_4(s_1, o_1, \underline{w})$ 和 $rq_5(s_1, o_1, \underline{w})$. 在传统的 BLP 模型中, 若 s_1 为非可信主体, 则执行结果是 rq_1 被允许, 而 rq_2~rq_5 被拒绝; 若 s_1 为可信主体, 则执行结果是 rq_1~rq_5 均被允许. 在示例的 CBLP 系统中, 数据请求的执行结果与传统 BLP 模型有所不同, 具体情况如表 2 所示:

表 2 系统对 rq_1~rq_5 数据请求的执行结果

	f_s	f_c	f_o	g_s^*/g_s^M	g_o^*/g_o^M	g_r/g_r^M	d	g_s 新值
rq_1	2	2	2	1.00/0.80	1.00/0.70	1.00/0.80	yes	1.00
rq_2	2	2	1	0.94/0.80	0.94/0.60	0.94/0.80	yes	0.94
rq_3	2	2	3	0.75/0.80	0.75/0.80	0.81/0.80	no	0.94
rq_4	2	2	1	0.82/0.80	0.82/0.60	0.88/0.80	yes	0.82
rq_5	2	2	1	0.63/0.80	0.63/0.60	0.77/0.80	no	0.82

由系统对 rq_1 的判断结果可看出, 主体在遵守 ss-属性和* -属性的前提下访问客体, 不会降低其可信度. 而在同一系统状态下对 rq_3 和 rq_4 的不同判断结果, 说明系统可对不同的客体实施严格程度不同的访问控制措施. 在不同系统状态下对相同数据请求 rq_2、rq_4 和 rq_5 的不同判断结果表明, 系统对数据请求的判断随着相应主客体可信度的变化而动态地改变. 如果修改式(5)中的 k 值为 0.2($x=\underline{r}/\underline{a}$)和 0.3($x=\underline{w}$), 系统对 rq_3 的可信度评估结果则为($g_r=0.86$, $g_s^*=0.82$, $g_o^*=0.82$), 系统将允许在当前参数设置中被拒绝的 rq_3 数据请求. 显然, 把系统的 g_r^M 值修改为 0.70 也能使 rq_3 数据请求得到执行.

3 结论

本文提出的 CBLP 多级安全访问控制模型, 以主客体的可信度标记为基础, 采用了相应的可信度评估函数对可信主体的可信度进行量化, 从而能够定量地评估可信主体在系统中真实的可信程度. 以此评估机制为基础, 建立了对可信主体的约束机制, 使系统可以赋予更多的主体有限程度的特权.

与传统 BLP 模型赋予可信主体无限的违规特权但对非可信主体严格执行"无上读, 无下写"规则的控制方式不同, CBLP 模型利用主体可信度阈值的设定实现了系统中可信主体和非可信主体的统一管理, 较好地解决了当前基于安全标记的多级安全系统中存在的可信主体安全隐患和系统可用性较差的问题. 同时, CBLP 模型可以通过修改主客体可信度阈值或可信度评估函数的方式修改模型的严格程度, 能够较好地应用于需要在可用性和安全性之间做出折中的应用系统中.

参考文献:

[1] Bell D E, LaPadula L J. Secure Computer System: Unified Exposition and Multics Interpretation[R]. MTR-2997, Bedford, MA: MITRE Corporation, 1976.

[2] Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations[R]. MTR-2547 Volume I, Bedford, MA: Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973.

[3] Bell D E, LaPadula L J. Secure Computer Systems: A Mathematical Model[R]. MTR-2547 Volume II, Bedford, MA: Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973.

[4] Bell D E. Secure computer systems: A network interpretation [A]. Proceedings of the 3rd Annual Computer Security Application Conference[C]. Vienna, VA, USA, 1987. 32- 39.

[5] Lee T M P. Using mandatory integrity to enforce "commercial" security[A]. Proceedings of the 8th National Computer Security Conference[C]. Gaithersburg, MD, USA, 1985. 108- 119.

[6] 季庆光, 卿斯汉, 贺也平. 一个改进的可动态调节的机密

性策略模型[J]. 软件学报, 2004, 15(10): 1547- 1557.
Ji Qing-guang, Qing Si-Han, He Ye-ping. An improved dynamically modified confidentiality policies model[J]. Journal of Software, 2004, 15(10): 1547- 1557. (in Chinese)

[7] 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): 1366- 1372.
Shi Wen-chang, Sun Yu-fang, Liang Hong-liang. An adaptable labeling enforcement approach and its correctness for the classical BLP security axioms[J]. Journal of Computer Research and Development. 2001, 38(11): 1366- 1372. (in Chinese)

[8] Trusted Information System Inc. Trusted Mach Mathematical Model[R]. TIS TMACH EDOG-0017-96B, Trusted Information System Inc, 1996.

作者简介:

谭智勇　男, 1979 年生于四川成都, 清华大学计算机科学与技术系博士生, 主要研究方向为多级安全模型和网络信息安全.
E-mail: tanzy05@mails.tsinghua.edu.cn

刘　铎　男, 1978 年生于北京, 清华大学计算机科学与技术系博士后, 博士, 主要研究方向为公钥密码学、组合算法的设计与分析.

司天歌　男, 1977 年生于辽宁阜新, 清华大学计算机科学与技术系博士生, 主要研究方向为网络信息安全.

戴一奇　男, 1946 年生于浙江瑞安, 清华大学计算机科学与技术系教授, 博士生导师, 主要研究方向为网络信息安全.