第7卷第2期
1996年2月

软 件 学 报
JOURNAL OF SOFTWARE

Vol. 7, No. 2
Feb. 1996

一个用于授权传递的改进Bell—La Padula模型*

洪 帆　余祥宣

(华中理工大学计算机科学与工程系　武汉　430074)

摘要　本文简要介绍用于安全计算机系统的Bell—La Padula模型.针对数据库系统中授权的可传递性,提出了一个基于Bell—La Padula模型的改进模型.改进模型对原模型的元素进行了扩充,对原模型的系统状态、公理及状态转换规则进行了改造,并给出和证明了其主要的结论.

关键词　授权传递,主体,客体,系统状态,公理,状态转换规则.

美国国防部于1983年发布了"可信计算机系统评估准则"[1],其中B2级以上要求有形式化的模型.由Bell D E和La Padula L J开发的Bell—La Padula(以下简称BLP)模型是最早的安全模型之一,已被许多安全操作系统采用作为其形式化安全模型.

BLP模型的安全策略包括两部分:自主安全策略和强制安全策略.它将主体对客体的访问分为r(只读),w(读写),a(只写),e(执行)以及c(控制)等几种访问模式.自主安全策略使用一个访问矩阵来表示,访问矩阵第i行第j列的元素M_{ij}表示主体s_i对客体o_j的所有允许的访问模式,主体只能按照在访问矩阵中被授予的对客体的访问模式对客体进行相应的访问.强制安全策略包括简单安全性和*_性质,系统对所有的主体和客体都分配有一个访问类属性,它包括主体或客体的密级和类别集.系统通过比较主体与客体的访问类属性来控制主体对客体的访问.[2]

在BLP模型中,主体对客体的"c",即"控制"访问权限是集中管理且不能扩展.一个主体只有在创建某个客体的时候,才能获得对这个客体的"c"权.主体s_i对客体o_j若具有"c"权,则s_i可以将它对o_j的所有其它访问权限授予系统中任何一个主体,但不能授予"c"权,s_i也可以撤销系统中任何主体对o_j的其它访问权,只要s_i对o_j同时具有这一访问权.若s_i对o_j不具有"c"权,即使s_i对o_j可能具有其它所有的访问权,s_i也无权授予或撤销其它主体对o_j的任何访问权.因此,一般情形下,对于客体o_j哪些主体可以对其进行访问,可以进行什么样的访问,在自主访问控制中,完全由o_j的拥有者决定.

尽管后来Bell D E对BLP模型中的"控制"权的管理作了改进[3],将主体对客体o_j的访

---

* 本文是国家自然科学基金资助项目.作者洪帆,1942年生,女,副教授,主要研究领域为计算机安全,密码学.余祥宣,1942年生,教授,主要研究领域为计算机安全,计算机算法.

本文通讯联系人:洪帆,武汉430074,华中理工大学计算机科学与工程系

本文1995—07—11收到修改稿

问控制权隐含在对 o_j 的父结点客体的"w"访问权中,使得控制权得以分散,但这种改进是为了适应Multics一类操作系统的要求,不能适用于数据库系统中授权传递的要求.在关系数据库系统中,对访问控制权的管理上,除了表的拥有者可以授予其它主体对该表的访问权外,往往还允许其它主体也具有对该表的访问权的授予权.[4]

因此,对于一个客体 o_j 的访问权,不仅 o_j 的拥有者可以授权,其它的主体也有可能得到全部或部分的授予权,只要有其它的主体授予它这种权利.相应地,一个主体在撤销它所授予的对某个客体的某种权限时,必须将由于这一授权而引起的所有的授权都予以撤销.为了描述数据库中对客体访问权限的授予与撤销上的这种可传递性,BLP模型的访问矩阵已显得无能为力.本文对BLP模型的元素进行扩充,对自主访问控制的矩阵模型进行改造,引进授权函数,动态地描述主体对客体的访问权限及主体对客体的访问授权路径,使改进后的模型能适用于描述系统中的授权传递.

1　BLP模型

BLP模型是一个状态机模型,它形式化地定义了系统、系统状态及状态间的转换规则,定义了安全的概念.并制定了一组安全特性,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,如果它的初始状态是安全的,并且所经过的一系列规则都是保持安全的,那么可以证明该系统是安全的.

1.1　系统状态

状态是系统中元素的表示.它由主体、客体、访问属性、访问矩阵以及标识主体和客体的访问类属性的函数组成.状态由一个有序三元组(b,M,f)所定义,其中 $b\subseteq(S\times O\times A)$,$S$ 是主体集,O 是客体集,$A=\{\underline{r},\underline{w},\underline{a},\underline{e},\underline{c}\}$是访问属性集.$b$ 表示在某个特定的状态下,哪些主体以何种方式访问哪些客体.M 是访问矩阵,其中元素 $M_{ij}\subseteq A$ 表示主体 S_i 对客体 O_j 具有的访问权限,$f\in F$ 为访问类函数,记作(f_1,f_2,f_3,f_4),其中 $f_1(s)$和 $f_3(s)$分别表示主体 s 的密级和类别集,$f_2(o)$和 $f_4(o)$分别表示客体 o 的密级和类别集.

1.2　状态转换规则

系统状态的转换由一组规则所定义,规则定义为函数 $\rho:R\times V\to D\times V$,其中 R 为请求集,D 为判断集,V 为状态集.规则 ρ 说明对于一个状态和一个请求,系统产生的判断和下一个状态,D 的取值范围为集合$\{\underline{Yes},\underline{No},\underline{?},\underline{Error}\}$,"$\underline{Yes}$"表示请求被执行,"$\underline{No}$"表示请求被拒绝,"$\underline{?}$"表示规则 ρ 不能处理这一请求,"$\underline{Error}$"表示有多个规则适用于这一请求—状态对.模型定义了10条规则,规则1～4用于主体对客体的访问请求;规则5用于主体释放对客体的访问,规则6和7分别用于主体授予和撤销另一主体对某一客体的访问权限;规则8用于改变死亡客体的密级和类别集;规则9和10分别用于创建和删除(使之成为死亡)一个客体.

1.3　系　统

设 $\omega=\{\rho_1,\rho_2,\cdots,\rho_s\}$是一组规则集,关系 $W(\omega)\subseteq R\times D\times V\times V$ 定义为:

(1)$(R_k,\underline{?},v,v)\in W(\omega)$ *iff* 对每个 i,$1\leqslant i\leqslant s$,$\rho_i(R_k,v)=(\underline{?},v)$;

(2)$(R_k,\underline{Error},v,v)\in W(\omega)$ *iff* 存在 i_1,i_2,$1\leqslant i_1<i_2\leqslant s$,使得对任意 $v^*,v^{**}\in V$,有 ρ_{i_1}

$(R_k,v)\neq(\underline{?},v^*)$且$\rho_{i_2}(R_k,v)\neq(\underline{?},v^{**})$；

(3)$(R_k,D_m,v^*,v)\in W(\omega)$,$D_m\neq\underline{?}$,$D_m\neq\underline{Error}$ *iff* 存在唯一的i,$1\leqslant i\leqslant s$,使得对某个$v^*\in V$和任意的$v^{**}\in V$,$(\underline{?},v^{**})\neq\rho_i(R_k,v)=(D_m,v^*)$；

设T是正整数集,X是所有请求序列集,Y是所有判断序列集,Z是所有状态序列集,系统$\Sigma(R,D,W,Z_0)$定义为:$\Sigma(R,D,W,Z_0)\subseteq X\times Y\times Z$,对任意$(x,y,z)\in X\times Y\times Z$,$(x,y,z)\in\Sigma(R,D,W,Z_0)$ *iff* 对于任一$t\in T$,$(x_t,y_t,z_t,z_{t-1})\in W$,其中$z_0$是初始状态.

1.4 模型的公理

BLP模型制定了一组公理(特性),其中主要有

(1)简单安全性:状态$v=(b,M,f)$满足简单安全性 *iff* 对所有的$(s,o,\underline{x})\in b$,(i)$\underline{x}=\underline{e}$或$\underline{x}=\underline{a}$或$\underline{x}=\underline{c}$,或(ii)($\underline{x}=\underline{r}$或$\underline{x}=\underline{w}$)且$(f_1(s)\geqslant f_2(o),f_3(s)\supseteq f_4(o))$.

(2)性质:*_状态$v=(b,M,f)$满足*_性质 *iff* 对所有的$s\in S$,若$b(s:\underline{w},\underline{a})\neq\varphi$且$b(s:\underline{r},\underline{w})\neq\varphi$,则$o_1\in b(s:\underline{w},\underline{a})$,$o_2\in b(s:\underline{r},\underline{w})$蕴含$f_2(o_1)\geqslant f_2(o_2)$且$f_4(o_1)\supseteq f_4(o_2)$.

其中符号$b(s:\underline{x_1},\ldots,\underline{x_n})$表示$b$中主体$s$对其具有访问权限$\underline{x_i}$($1\leqslant i\leqslant n$)的所有客体集合.

(3)自主安全性:状态$v=(b,M,f)$满足自主安全性 *iff* 对所有的$(s_i,o_j,\underline{x})\in b$,$\underline{x}\in M_{ij}$.

(4)激活公理:为简化M和f结构,BLP模型认为所有在系统中使用过的客体都已存在,一个新客体的创建是一个不活跃客体的激活,一个客体的删除是一个活跃客体的死亡.

2 改进模型

2.1 模型元素的扩充和改造

在BLP模型中引入集合:$S^*=\{s_{t_1}s_{t_2}\cdots s_{t_r}\mid s_{t_j}\in S,j=1,2,\cdots,r,r\in N\}$,其中$N$是正整数集.$S^*$是$S$中有限个主体所构成的序列的集合,序列可以为空.

$M\cdot S^*=\{ms^*\mid s^*\in S^*\}$是授权路径集,$m$代表系统.

$G\cdot S^*=\{Gs^*\mid s^*\in S^*\}$是被授权主体序列集,$G$表示授予权.

$H=G\cdot S^*\cup\{N\}$,H中的元素用h表示,N表示无授予权.

将BLP模型中的访问属性集A修改为$A=\{\underline{r},\underline{w},\underline{a},\underline{e}\}$,控制权$\underline{c}$通过$G$和$N$来表示.

定义授权函数$g:S\times O\times A\to P(M\cdot S^*\times H)$,$P(M\cdot S^*\times H)$是$M\cdot S^*\times H$的幂集.

对于任一$(s_i,o_j,\underline{x})\in S\times O\times A$.

若$g(s_i,o_j,\underline{x})=\varphi$,表示主体$s_i$对客体$o_j$不具有$\underline{x}$访问权.

若$g(s_i,o_j,\underline{x})=\{(ms_1^*,h_1),(ms_2^*,h_2),\cdots,(ms_n^*,h_n)\}$,表示有$n$条授权路径$ms_1^*,ms_2^*,\cdots,ms_n^*$,分别授予了主体$s_i$对客体$o_j$的$\underline{x}$访问权,对每一个$h_k$($1\leqslant k\leqslant n$),若$h_k=G$,表示$ms_k^*$,不但授予了$s_i$对$o_j$的$\underline{x}$访问权,并且授予了$s_i$对该访问权的授予权.若$h_k=Gs_{t_1}s_{t_2}\cdots s_{t_r}$,表示$s_i$已将从$ms_k^*$得到的对$o_j$的访问权$\underline{x}$依次授予了主体$s_{t_1},s_{t_2},\cdots,s_{t_r}$.若$h_k=N$,表示$ms_k^*$仅授予了$s_i$对$o_j$的$\underline{x}$访问权,$s_i$不具有对该权的授予权.

若对于$\forall s\in S$和$\forall\underline{x}\in A$,均有$g(s,o_j,\underline{x})=\varphi$,则记作$g(S,o_j,A)=\varphi$,这表明$o_j$是一个死亡客体.用授权函数$g$代替BLP模型中的访问矩阵进行自主访问控制.

对$P(M\cdot s^*\times H)$中的元素定义如下的运算:

运算+:对任意$\beta\in P(M\cdot S^*\times H)$和任意$(ms_k^*,s_{t_i})\in M\cdot S^*\times S$,$\beta+(ms_k^*,s_{t_i})$表示对

β中序偶(ms_k^*,h_k)的h_k添加s_{t_i}使之成为序偶$(ms_k^*,h_ks_{t_i})$.

运算$-$:对任意$\beta\in P(M\cdot S^*\times H)$和任意$(ms_k^*,s_{t_i})\in M\cdot S^*\times S$,$\beta-(ms_k^*,s_{t_i})$表示从$\beta$中序偶$(ms_k^*,h_k)$的$h_k$中删除$s_{t_i}$,$h_k$中其它主体保持不变.

运算$\odot$:对任意$\beta\in P(M\cdot S^*\times H)$和任意$(ms_k^*,h)\in M\cdot S^*\times H$,$\beta\odot(ms_k^*,h)$表示若$\beta$中有以$ms_k^*$为第一坐标的序偶,则将其从$\beta$中删除.

2.2 模型状态及公理的改造

定义系统状态$v=(b,g,f)$,其中$b\subseteq S\times O\times A$仍为当前访问集,$f$仍为访问类函数,$g$是授权函数,表示主体对客体的访问权及访问授予权.

改进模型的自主安全性叙述如下:状态$v=(b,g,f)$满足自主安全性iff对所有的$(s_i,o_j,\underline{x})\in b$,$g(s_i,o_j,\underline{x})\neq\varphi$.

2.3 模型规则的改造

将原模型规则中的自主安全性检查修改为:

$$\text{if } g(s_i,o_j,\underline{x})=\varphi \text{ then } \rho_i(R_k,v)=(\underline{no},v)$$

便得到改进模型的规则1～4,原模型的规则5和规则8不涉及自主安全性检查,只要用授权函数g取代访问矩阵即可得到改进模型的规则5和规则8.

为描述改进模型中的规则6,规则7,规则9和规则10,令请求集

$$R=S^+\times RA\times S^+\times O\times X\times Q\times P$$

其中仍有$S^+=S\cup\{\varphi\}$,$RA=\{g,r,c,d\}$为请求元素集,$X=A\cup\{\varphi\}\cup F$.这里,定义$Q=M\cdot S^*\cup\{\varphi\}$,$P=\{G,N\}\cup\{\varphi\}$.

R的元素R_k表示为$(\sigma_1,\gamma,\sigma_2,o_j,\underline{x},\sigma_3,p)$,若$\sigma_1\in S$,则记作"$s_\lambda$",若$\sigma_2\in S$,则记作"$s_i$",若$\sigma_3\in M\cdot S^*$,则记作$ms_\delta^*$.

规则6:*give_read/write/append/execute*:$\rho_6(R_k,v)\equiv$

if $(\sigma_1\neq s_\lambda\in S)$ or $(\gamma\neq g)$ or $(\sigma_2=\varphi)$or$(\underline{x}\neq\underline{r},\underline{w},\underline{a}$ and $\underline{e})$

or$(\sigma_3\neq ms_\delta^*\in M\cdot S^*)$

then $\rho_6(R_k,v)=(\underline{?},v)$;

if $(ms_\delta^*,h)\in g(s_\lambda,o_j,\underline{x})$ and $h\neq N$

then

if $p=G$ then $\rho_6(R_k,v)=(\underline{yes},(b,g^*=g(g(s_i,o_j,\underline{x})\cup\{(ms_\delta^*s_\lambda,G)\},g(s_\lambda,o_j,\underline{x})+(ms_\delta^*,s_i)),f))$;

if $p=N$ then $\rho_6(R_k,v)=(\underline{yes},(b,g^*=g(g(s_i,o_j,\underline{x})\cup\{(ms_\delta^*s_\lambda,N)\},g(s_\lambda,o_j,\underline{x})+(ms_\delta^*,s_i)),f))$;

else $\rho_6(R_k,v)=(\underline{no},v)$

end.

规则7:*rescind_read/write/append/execute*,$\rho_7(R_k,v)\equiv$

if $(\sigma_1\neq s_\lambda\in S)$ or $(\gamma\neq r)$ or $(\sigma_2=\varphi)$ or $(\underline{x}\neq\underline{r},\underline{w},\underline{a}$ and $\underline{e})$

or$(\sigma_3\neq ms_\delta^*\in M\cdot S^*)$ or $(p\neq\varphi)$

then $\rho_7(R_k,v)=(\underline{?},v)$;

if $(ms_\delta^*, h) \in g(s_\lambda, o_j, \underline{x})$ and $h = Gs^*$ and $s_i \in s^*$

then $g^* = g(g(s_\lambda, o_j, \underline{x}) - (ms_\delta^*, s_i), g(s_i, o_j, \underline{x}) \odot (ms_\delta^* s_\lambda, h), g(s, o_j, \underline{x}) \odot (ms_\delta^* s_\lambda s_i s^*,$
$h)$ for $\forall s \in S, \forall s^* \in S^*)$,

$b^* = b - \{(s_t, o_j, \underline{x})\}, s_t \in \{s \mid g^*(s, o_j, \underline{x}) = \varphi\}$,

$\rho_7(R_k, v) = (\underline{yes}, (b^*, g^*, f))$;

else $\rho_7(R_k, v) = (\underline{no}, v)$

end.

规则 9: $Create-object: \rho_9(R_k, v) \equiv$

if $(\sigma_1 \neq \varphi)$or$(\gamma \neq c)$or$(\sigma_2 \neq s_i \in S)or(\underline{x} \neq \underline{e}$ and $\varphi)$or$(\sigma_3 \neq \varphi)$or$(p \neq \varphi)$

then $\rho_9(R_k, v) = (\underline{?}, v)$;

if $g(S, o_j, A) \neq \varphi$ then $\rho_9(R_k, v) = (\underline{no}, v)$;

if $\underline{x} = \varphi$ then $\rho_9(R_k, v) = (\underline{yes}, (b, g^* = g(g(s_i, o_j, \underline{x}) \cup \{(m, G)\}_{\underline{z}=\underline{r}, \underline{a}, \underline{w}}), f))$

else $\rho_9(R_k, v) = (\underline{yes}, (b, g^* = g(g(s_i, o_j, \underline{x}) \cup \{(m, G)\}_{\underline{x}=\underline{r}, \underline{a}, \underline{w}, \underline{e}}), f))$

end.

规则 10: $Delete-object: \rho_{10}(R_k, v) \equiv$

if $(\sigma_1 \neq \varphi)$or$(\gamma \neq d)$or$(\sigma_2 \neq s_i \in S)or(\underline{x} \neq \varphi)or(\sigma_3 \neq \varphi)or(p \neq \varphi)$

then $\rho_{10}(R_k, v) = (\underline{?}, v)$;

if $(m, h) \in g(s_i, o_j, \underline{x})$ for some $\underline{x} \in A$

then $\rho_{10}(R_k, v) = (\underline{yes}, (b, g^* = g(g(S, o_j, A) = \varphi), f))$

else $\rho_{10}(R_k, v) = (\underline{no}, v)$

end.

上述规则描述中的 $g^* = g(\alpha)$ 表示 g^* 由对 g 进行 α 所指定的操作而得到.

3 结 论

结论 1. 在改进模型中,对客体的访问实现了由其拥有者自主决定的授权及授权的可传递性,允许循环授权. 撤销授权时,可按照授权路径给予正确的撤销.

说明:由改进模型的规则 9 和规则 6 可以看出,当一个主体创建某个客体时,该主体便获得对这一客体的所有访问权,包括访问的授予权. 其它的主体只有在得到授权后,才能对该客体进行访问,且只有被授予了授予权后,方可对相应的访问权进行授权. 由规则 7 可以看出,撤销授权时按授权路径进行搜索予以撤销. 因为授权和撤销授权均按授权路径进行,所以当有循环授权时,亦能正确撤销.

结论 2. 设 $\omega = \{\rho_1, \rho_2, \cdots, \rho_{10}\}$, z_0 是一安全状态,则改进模型所定义的系统 $\Sigma(R, D, W(\omega), z_0)$ 是安全的.

证明:将使用规则前的状态记作 $v = (b, g, f)$,使用规则后的状态记作 $v^* = (b^*, g^*, f^*)$. 因为改进模型仅对 BLP 模型的自主安全性进行改造,BLP 模型的简单安全性和 * -性质等公理仍然适用,所修改的状态转换规则均使得 $b^* \subseteq b, f^* = f$,因此所有状态转换规则仍是安全性保持和 * -性质保持的,又因 z_0 是安全的,所以改进模型所定义的系统是安全的.

参考文献

1 U S Department of Defense. DOD trusted computer system evaluation criteria. DOD5200.28—std, Washington, D.C.: Department of Defense, 1985.

2 Bell D E, La Padula L J. Secure computer system: a mathematical model. ESD—TR—73—278, Vol. Ⅰ, Bedford, Mass.: Mitre Corp., 1973.

3 Bell D E. Secure computer system: a refinement of the mathematical model. ESD—TR—73—278, Vol. Ⅱ, Bedford, Mass.: Mitre Corp., 1973.

4 Denning D E. Cryptography and data security. Reading, Mass.: Addison—Wesley, 1982.

AN IMPROVED Bell—La Padula MODEL FOR THE TRANSFER OF AUTHORIZATION

Hong Fan　Yu Xiangxuan

(*Department of Computer Science and Engineering　Huazhong University of Science and Technology　Wuhan* 430074)

Abstract　This paper first describes briefly the Bell—La Padula model used for secure computer system. Then an improved Bell—La Padula model is proposed according to the transferability of authorization of database system. It extends the elements of the original model and reforms the state of system, axioms and rules for state transition of the original model. The main conclusions of the improved model are presented and proved.

Key words　Transfer of authorization, subject, object, state of system, axiom, rule for transition.