一个修改 BLP 安全模型的设计及在 SecLinux 上的应用*

刘文清, 卿斯汉, 刘海峰

(中国科学院 软件研究所 信息安全技术工程研究中心,北京 100080)
E-mail: lwq@ercist.iscas.ac.cn
http://www.ercist.iscas.ac.cn

摘要: 建立了一个面向最小特权管理的修改 BLP 安全模型.该模型引入了角色管理、域隔离、隐蔽通道限制、病毒防护等概念,并实际应用于自主开发的安全操作系统 SecLinux 中.

关 键 词: 计算机安全模型;安全操作系统设计;最小特权管理;域隔离
中图法分类号: TP309 文献标识码: A

形式化的安全模型是设计开发高级别安全操作系统的前提.一个操作系统是安全的,是指它满足某一给定的安全策略,安全模型则是对安全策略所表达的安全需求简单、抽象和无歧义的描述.目前,人们只公认少数几个安全模型,用于实际系统的就更少了.

建立计算机安全模型是一项十分困难的工作,既要具备一定的条件,又需付出很大的努力才能完成.但对于安全操作系统开发者来说,可以对现有的几种安全模型作深入的研究,并面向自己的安全策略作修改,以满足安全需求[1,2],像 BLP 模型就已经成功地应用在许多安全系统的设计中.

1 BLP 模型

1.1 BLP模型简介

BLP(Bell-La Padula)模型是一个状态机模型[3~5],它由 David Bell 和 Leonard La Padula 于 1973 年创立,是模拟符合军事安全策略的计算机操作的模型,也是最早和最常使用的一种模型.它形式化地定义了系统状态及状态间的转换规则,并制定了一组约束系统状态间转换规则的安全公理.

(1) 系统状态

系统状态是集合 $V=(B\times M\times F\times H)$中的元素,其中 $B\subseteq(S\times O\times A)$为当前存取集,$S$ 为主体的集合,O 为客体的集合,A 为访问权限集合,它由以下元素组成:e(执行)、r(读)、a(追加写)、w(写)和-(空);M 为存取控制矩阵,它由元素 $m_{ij}\in A$ 组成,m_{ij} 表示主体 S_i 对客体 O_j 具有的访问权;F 为安全级函数,由以下 3 个分量组成:fm 为主体的最大安全级,fo 为客体的安全级,fs 为主体的当前安全级;H 为当前层次结构,即当前客体的树型结构.

系统任一状态 $v=(b,M,f,H)\in V$,其中 $b=(S_i,O_j,\underline{x})\in B,\underline{x}\subseteq m_{ij};f=(fm,fo,fs)\in F$.

(2) 状态转换规则

系统状态间的转换是由一组规则定义的,规则为函数,它说明对任意状态,输入(请求)所产生的下一状态及输入(判定).

* 收稿日期: 2000-07-03; 修改日期: 2000-12-05
基金项目: 国家自然科学基金资助项目(60083007);国家重点基础研究 973 发展规划资助项目(G1999035810);中国科学院知识创新工程资助项目(YC2K5609);
作者简介: 刘文清(1967－),男,河南虞城人,博士生,副研究员,主要研究领域为操作系统安全,网络安全;卿斯汉(1939－),男,湖南邵阳人,研究员,博士生导师,主要研究领域为信息系统安全理论与技术;刘海峰(1975－),男,山东泰安人,博士生,主要研究领域为信息系统安全理论与技术.

一个规则的定义为$\rho:R\times V\to D\times V$,$R\times V$ 为系统中“请求-状态对”集合,$D\times V$ 为系统中“判定-状态对”集合.R 为请求集,D 为判定集.判定的结果为(Yes,No,？)之一.“Yes”表示请求被执行,“No”表示请求被拒绝,“？”表示规则不能处理该请求.

规则ρ保持安全状态当且仅当$\rho(R_k,v)=(D_m,v^*)$,v 是安全状态时,有 v^*是安全状态.

(3) 安全公理

安全公理是构成 BLP 模型的基础,具体内容如下:

① 简单安全公理(simple security),又称 ss-特性:

状态 $v=(b,M,f,H)$满足 ss-特征,iff 对所有$(s,o,\underline{x})\in b$.

(i) $\underline{x}=a$ 或 $\underline{x}=e$;

(ii) $\underline{x}=w$ 或 $\underline{x}=r$,且 $fs(s)\geq fo(o)$.

② *特性公理(star property),又称*-特性:

状态 $v=(b,M,f,H)$满足*-特征,iff 对所有$(s,o,\underline{x})\in b$.

(i) $\underline{x}=a\Rightarrow fo(o)\geq fs(s)$;

(ii) $\underline{x}=w\Rightarrow fo(o)=fs(s)$;

(iii) $\underline{x}=r\Rightarrow fo(o)\leq fs(s)$.

这里,主体为不可信主体,*-特性对可信主体没有限制.

③ 自主安全公理(discretionary property),又称 ds-特性:

状态 $v=(b,M,f,H)$满足 ds-特征,iff 对所有$(s_i,o_j,x)\in b,x\in m_{ij}$.

(4) 基本安全定理

系统是安全系统,当且仅当初始状态是安全状态,且对每一次状态转变满足简单安全特性、*-特性和自主安全特性.

1.2 BLP模型分析

BLP 模型的安全策略包括强制存取控制和自主存取控制两部分.强制存取控制部分由简单安全特性和*-特性组成,通过安全级来强制性地约束主体对客体的存取;自主存取控制通过存取控制矩阵按用户的意愿来进行存取控制.

BLP 使用了可信主体的概念,用于表示在实际系统中不受*-特性制约的主体,以保证系统的正常运行和管理.

但随着计算机安全理论和技术的发展,BLP 模型已不足以描述各种各样的安全需求.应用 BLP 模型还应考虑以下几个方面的问题:

·在 BLP 模型中,可信主体不受*-特性约束,其访问权限太大,不符合最小特权原则,应对可信主体的操作权限和应用范围进一步细化.

·BLP 模型主要注重保密性控制,控制信息从低安全级传向高安全级,而缺少完整性控制,不能控制“向上写(write up)”操作,而“向上写”操作存在着潜在的问题,它不能有效地限制隐蔽通道[6].

2 MBLP 安全模型设计[7]

SecLinux 是我们基于现有 Linux 资源自主开发的安全操作系统,设计目标是达到我国 GB17859-1999《计算机信息系统安全保护等级划分准则》第 3 级.在进行 SecLinux 设计时,我们进行了安全模型的设计.SecLinux 的安全模型就是在对 BLP 分析的基础上,结合 SecLinux 的安全策略,并基于 BLP 安全模型修改建立的,我们记为 MBLP(modified BLP).

(1) MBLP 模型定义

定义 **1**. D 为域函数,它将 S 中的主体或 O 中的客体映射到相应的域中.对于主体来说,D 的定义域是 S,值域是$\{Su,St\}$,其中 Su 表示普通用户域或非特权域,代表系统一般用户的操作,St 表示可信用户域或特权域,代表系

统所有特权操作.对于客体来说,D 的定义域是 O,值域是{Ou,Os,Ov},其中 Ou 代表用户空间域,Os 代表系统空间域,Ov 代表病毒保护域.

定义 **2**. P 为特权映射函数,它将 St 映射到不同的项中.P 的定义域为 St,值域为{p_1,p_2,p_3,p_4,…,p_n},其中 $St=p_1\cup p_2\cup p_3\cup p_4\cup\ldots\cup p_n$.

定义 **3**. R 为角色映射函数,它将{p_1,p_2,p_3,p_4,…,p_n}映射到不同的集合中.R 的定义域为{p_1,p_2,p_3,p_4,…,p_n},值域为{P_1,P_2,P_3,…,P_m}.其中 $P_i=\{p_j|1\le j\le n\}$,$1\le i\le m$,我们把 P_i 又称为角色 i.

(2) MBLP 模型公理

① 域间隔离性

主体只能访问相应客体域中的客体.即,状态 $v=(b,M,f,H)$满足域间隔离性,iff 对所有$(s,o,\underline{x})\in b$.

(i) $\underline{x}=a$ 或 $\underline{x}=w$,且 $o\in Ou$,$s\in Su$,或,

(ii) $\underline{x}=r$,且 $o\in Ou\cup Ov$,$s\in Su$,或,

(iii) $\underline{x}=a$ 或 $\underline{x}=w$,且 $o\in Os$,$s\in St$,或,

(iv) $\underline{x}=r$,且 $o\in Os\cup Ov$,$s\in St$,或,

(v) $\underline{x}=a$ 或 $\underline{x}=w$,且 $o\in Ov$,$s\in P_n$,n 为一特定值,

(vi) $\underline{x}=a$ 或 $\underline{x}=w$,且 $o\in Ou$,$s\in P_m$,m 为一特定值.

② 简单安全公理

当一主体读访问一客体时,主体的安全级必须大于或等于客体的安全级,或主体拥有指定特权.即,状态 $v=(b,M,f,H)$满足简单安全公理,iff 对所有$(s,o,\underline{x})\in b$.

(i) $\underline{x}=a$ 或 $\underline{x}=e$ 或,

(ii) $\underline{x}=w$ 或 $\underline{x}=r$,且 $fs(s)\ge fo(o)$或 $s\in P_n$,n 为一特定值.

③ *特性公理

状态 $v=(b,M,f,H)$满足*特征公理,iff 对所有$(s,o,\underline{x})\in b$,$s\in\{Su\cup St\}$.

(i) $\underline{x}=w$ 或 $\underline{x}=a$,且 $fo(o)=fs(s)$,或 $s\in P_n$,n 为一特定值,

(ii) $\underline{x}=r$,且 $fo(o)\le fs(s)$或 $s\in P_n$,n 为一特定值.

④ 自主安全公理

状态 $v=(b,M,f,H)$满足自主安全公理,iff 对所有$(s_i,o_j,\underline{x})\in b$,$\underline{x}\in m_{ij}$.

⑤ 兼容性公理

客体层次结构 H 保持兼容性,iff 对$\forall o_i,o_j\in O$,且 $o_j\in H(o_i)$,有 $fo(o_j)\ge fo(o_i)$.

⑥ 激活性公理

用于约束 H 中客体的创建与删除.

(i) 已删除客体的不可存取性.即对所有已被删除的客体 $o\in O$,有$(s,o,*)\notin B$,

(ii) 新创建客体的重写性.即,一个新创建的客体被赋于一个与其以前任何活动状态无关的初始状态,

(iii) 新创建客体的安全级.对于每个被主体 s 创建的客体 o,有 $fo(o)=fs(s)$,

(iv) 客体删除规则.对于每个被主体 s 删除的客体 o,有 $fo(o)=fs(s)$.

(3) MBLP 模型主要推论

推论 **1**. 在 MBLP 模型中,对于普通用户域的主体 Su,BLP 模型的基本安全定理仍然成立.

证明:在 MBLP 模型中,对于普通用户域的任意主体 $s\in Su$,简单安全公理和自主特性公理与 BLP 模型完全一样,*-特性公理是 BLP 模型*-特性公理的特例(“写相等”是“向上写”的特例),并完全符合其条件要求(安全级相等条件成立就意味着支配条件成立).所以,BLP 模型的基本安全定理在 MBLP 模型中仍然成立.

推论 **2**. 在 MBLP 模型中,对于可信用户域的主体 St,满足二人原则(double control).

证明:在 MBLP 模型中,角色映射函数 R 将系统的所有特权操作 $St=p_1\cup p_2\cup p_3\cup p_4\cup\ldots\cup p_n$,映射到不同的角色中,并把这些“角色”赋于系统中的指定用户,这样,操作系统中就存在有若干个特权用户,这些特权用户共同完成系统的特权操作,每一个特权用户(角色)仅拥有完成其管理工作所需的最小特权,即仅能控制系统的部分

特权,而不能独自控制整个系统,且所有的特权用户操作都会被系统审计记录,审计操作是在其他特权用户无法干预的情况下进行的.所以,MBLP 模型满足二人原则.

推论 **3**. MBLP 模型可有效地实现应用型病毒防护.

证明:根据域间隔离性,主体只能写访问相应客体域中的客体.

对于病毒防护域的客体 Ov,有

(i) 当 $\underline{x}=r$ 时,$s\in Su\cup St$;

(ii) 当 $\underline{x}=a$ 或 $\underline{x}=w$ 时,$s\in P_n$,n 为一特定值.

即,只有拥有指定特权的主体,才可以在病毒防护域增加客体和对其客体进行修改操作.所以,MBLP 模型有效地阻止了应用型病毒的入侵和传染.

另外,用户空间域 Ou 和系统管理域 Os 的隔离,使得

(i) $\underline{x}=\varnothing$,且 $o\in Os$,$s\in Su$;

(ii) $\underline{x}=a$ 或 $\underline{x}=w$,且 $o\in Ou$,$s\in P_m$,m 为一特定值.

即,普通用户域的主体无法对系统管理域的客体操作,也就是说,普通用户域的操作将无法影响系统管理域的客体.另外,只有拥有指定特权的主体,才可以对用户空间域的客体进行操作.所以,MBLP 模型有效地限制了应用型病毒在域间的传染.

因此,MBLP 模型可有效地实现应用型病毒的防护.

推论 **4**. MBLP 模型可有效地限制隐蔽通道.

证明:见上述“BLP 模型分析”,遵循 BLP 模型的安全操作系统含有隐蔽通道.MBLP 模型则将其强制性安全规则修改成为

(1) if $CLASS(S)>=CLASS(O)$

then Read(S,O) or Execute(S,O);

(2) if $CLASS(S)==CLASS(O)$

then Write(S,O) or Append(S,O).

其中 $CLASS(S)$,$CLASS(O)$表示主体与客体的安全级.

这样,在保证 MBLP 模型保密性的基础上,加入了完整性条件,限制了隐蔽通道的发生.

3 MBLP 安全模型在 SecLinux 的应用

MBLP 安全模型建立之后,就要进行模型与 SecLinux 系统的对应性分析,然后考虑如何将 MBLP 模型用于 SecLinux 的开发之中,并且说明所建模型与安全策略二者是一致的.由于 MBLP 模型与 SecLinux 安全策略的一致性是明显的,下面着重讨论 MBLP 模型的主要内容,包括系统状态、状态转换、安全初始状态定义以及安全公理系统在 SecLinux 中的对应.SecLinux 是基于 Linux 资源采用“改进/增强法”开发的安全操作系统,其文件系统是在原 ext2 文件系统基础上扩充的,并保持与其兼容性.其他,如进程系统、信号(中断)系统等,与 Linux 是基本一致的.因此,这里不再赘述.

(1) MBLP 模型的系统状态在 SecLinux 中的对应

系统状态同样是集合 $V=(B\times M\times F\times H)$中的元素.

在 SecLinux 中进程是惟一的主体,它可以在用户登录时创建、被系统初启时创建或被其他进程创建.一个进程被赋予一个惟一的进程标识符(pid)、用户标识符(uid)和用户组标识符(gid).每个进程还被赋予相应的安全级标识,用于强制存取控制检查.

在 SecLinux 中,客体包括文件、目录、特别文件、共享内存、消息、信号量、流、管道、进程.

MBLP 的访问权限集与 BLP 一样,由 e(执行)、r(读)、a(追加写)、w(写)和-(空)组成,SecLinux 的访问权限集则由读(r)、写(w)、执行(x)和空(-)组成,但它们对不同的客体有不同的解释,具体见表 1.

SecLinux 的当前访问集 B 是 $S\times O\times A$ 的子集,对于文件、目录、特别文件、管道等具有文件系统的数据结构表示的客体,B 由每个进程打开文件的文件描述符及其对应的访问权限表示.这些文件描述符存放于进程 task

结构中,其中的每个文件描述符指向文件表中的一项,记录了该进程对某客体具有的访问权限.对于 IPC 机制的客体,*B* 由每种类型客体的数据结构表示.进程获取的每个描述符指向一类客体的索引项,其中的 ipc_perm 项记录着该进程对该客体具有的访问权限.

SecLinux 的存取控制矩阵 M 有与每个 Linux 相对应的 9bit 位保护模式(owner/group/other)和 ACL(access control list)共同组成,表示客体主允许其他用户如何共享他的客体.

Table 1 SecLinux access mode set

表 **1** SecLinux 的访问权限集

MBLP	File	Dir	FIFO	IPC	Process
r	-	-	-	-	-
r	r	x	r	R	r
re	x	-	-	-	-
a	w	w	w	w	-
w	rw	w	rw	rw	w
-	-	-	-	-	-

SecLinux 的安全级函数 *F* 由两部分组成,一是每个进程被赋予的一个当前安全级,另一个是每个客体被赋予的一个确定的安全级.安全级由级别和类别两部分组成,如机密,{人事,军队}.

SecLinux 中具有文件系统表示的客体结构 *H* 是由目录表示的.具有文件系统表示的客体类型有文件、特别文件、有名管道和目录.文件、特别文件和有名管道的安全级等于其创建进程的安全级,且等于包含它们的父目录的安全级,目录的安全级也等于其创建进程的安全级,且大于或等于包含它的父目录的安全级,维持了目录结构的“不降级”.

(2) MBLP 模型的状态转换在 SecLinux 中的对应

SecLinux 的状态转换是由内核调用及其返回值定义的,对于 MBLP 模型规则集的任一规则ρ:$R\times V\to D\times V$ 中的任一规则ρ_i 有:

① 任意请求 $R_k\in R$ 表示一个指定的系统调用或可信进程调用.*R* 为所有系统调用和可信进程调用的集合,R_k 的输入参数则来自于当前系统状态 *V*.

② 任一判定 $D_m\in D$={Yes,No,?,Error}由一个系统调用或可信进程调用的返回值表示.

③ 无论何时,若 $D_m\neq$No,$D_m\neq$?,$D_m\neq$Error,R_k 则输出一个新状态 *v**,它将包含新的客体和一个新的客体结构,当然也可以从以前状态中排除某些客体和访问权限等.

④ 规则ρ保持了系统的安全状态,即当 *v* 是安全状态时,有 *v**是安全状态.这由 MBLP 模型的安全公理系统及其操作规则来保障.

(3) MBLP 模型的安全公理系统在 SecLinux 中的对应

① SecLinux 的域间隔离性

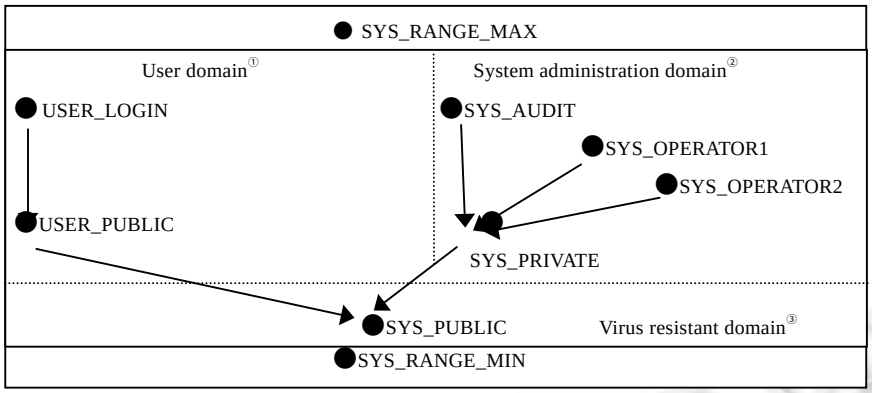
SecLinux 安全操作系统用安全级将系统信息划分成 3 个区,即系统管理区、用户空间区、病毒保护区.如图 1 所示,该图可看做是一组系统安全级和用户安全级,它们通过 MAC 机制的控制被分隔.其中,“箭头”表示安全级支配关系.

系统管理区不能被用户读和写,如可信计算基(TCB)数据、审计信息等,这样,TCB 使用访问隔离的方法进行自我保护,保护自身的安全性可以使 TCB 可信,正如它保护安全系统中所有其他可信部分一样.

用户空间区包含用户的数据和应用,用户可以进行读和写.

病毒保护区包含不能被用户区的进程写的数据、文件,但可被用户区的进程读.

这样的访问隔离机制将进入系统的用户划分为两类:不具有特权的普通用户,他们在用户空间区中的安全级(如 USER_LOGIN 或 USER_PUBLIC)下登录,系统管理员在系统管理区中的安全级(如 SYS_AUDIT, SYS_OPERATOR1,SYS_OPERATOR2 或 SYS_PRIVATE)下登录.



①用户空间区,②系统管理区,③病毒防护区.

Fig.1 SecLinux domain separation via system security levels

图 1 SecLinux 的系统安全级域隔离

② 强制存取控制 MAC(mandatory access control)规则

(a) 若主体读(r)或执行(x)访问客体,主体的安全级必须支配客体的安全级,或主体拥有 CAP_MACREAD 特权,记为 **R1**.

(b) 若主体写(w)访问客体,主体的安全级必须等于客体的安全级,或主体拥有 CAP_MACWRITE 特权,记为 **R2**.

③ 自主存取控制 DAC(discretionary access control)规则

(c) 若进程以 $\underline{x}$ 权限访问客体,$\underline{x}$ 须在客体的相应 ACL 项中,即 $\underline{x} \subseteq m_{ij}$,记为 **R3**.

④ 特权管理 PAC(privileged access control)规则

(d) 若主体写(w)访问客体的 ACL,主体的安全级必须等于客体的安全级或主体拥有 CAP_MACWRITE 特权,且主体须与客体主的用户标识符相匹配或主体拥有 CAP_OWNER 特权,记为 **R4**.

(e) 若主体写(w)访问客体的安全级,主体的安全级必须等于客体的安全级或主体拥有 CAP_MACWRITE 特权,且主体必须拥有 CAP_SETLEVEL 特权,记为 **R5**.

(f) 若主体执行特权操作时,主体的当前特权集必须拥有相应的特权,记为 **R6**.

⑤ 兼容性规则

(g) 若主体创建文件类型的客体时,客体的安全级必须等于其所在父目录的安全级,记为 **R7**.

(h) 若主体创建目录类型的客体时,客体的安全级必须支配其所在父目录的安全级,记为 **R8**.

⑥ 激活性规则

(i) 若主体创建客体时,新客体的安全级等于主体的安全级,记为 **R9**.

(j) 若主体删除客体时,主体的安全级必须等于客体的安全级或拥有 CAP_MACWRITE 特权,且在客体的 ACL 中,主体对客体和客体所在的目录拥有写权限,记为 **R10**.

(k) 删除一个客体时,其敏感信息,包括 ACL、安全级、特权集等均在客体删除之前删除,记为 **R11**.

(4) SecLinux 的最小特权管理

SecLinux 将原 Linux 超级用户(root)的特权分解成 32 个特权元素,初始安装时,系统将它们缺省组合成 4 个特权集合(角色),即系统安全管理员、系统安全操作员、系统安全审计员和网络管理员,赋于了 4 个不同用户.当然,原则上可以根据需要任意组合特权角色,但必须使每一个特权用户,仅拥有完成其管理工作所需的最小特权.代表特权用户工作的进程所具有的特权及进程之间的特权传递则是通过计算完成的.

(5) SecLinux 的安全初始态

SecLinux 安全操作系统的安全初始态由一个安全初始化过程设置,包括以下 4 个步骤:

✧ 系统的构造和生成,包括审计机制、MAC 机制、DAC 机制和 PAC 机制的安装和初始化;

✧ 系统中用户安全文件档的定义,即根据安全策略给系统中每个用户赋予相应的安全级库、角色划分;

✧ 系统中客体初始安全级设置,即系统用户空间区、系统管理区、病毒防护区等的划分及建立;

✧ 系统正常启动.

4 结束语

操作系统的安全是整个计算机系统安全的基础,没有操作系统安全,就不可能真正解决数据库安全、网络安全和其他应用软件的安全问题.虽然在这个领域我国与国外相比差距很大,但现在,开发一个安全的操作系统或提高现有主流操作系统的安全性已逐渐成为研究的热点.

目前,我们已将 MBLP 安全模型实际应用于自主开发的安全操作系统 SecLinux 中,相信 SecLinux 的成功开发将会对我国操作系统安全以及自主操作系统的研究与开发具有重要意义.

References:

[1] Millen, J.K., Cerniglia, C.M. Computer security models. MTR-9531. Bedford, MA.: Mitre Corp., 1984.

[2] Landwehr, C.E. Formal model for computer security. Computer Surveys, 1981,13(3):247~278.

[3] Bell, D.E., La Padula, L.J. Secure computer systems: mathematical foundations. ESD-TR-73-278, Ⅰ(AD)770 768, Electronic Systems Division, Air Force System Command, Hanscom AFB, Bedford, MA, 1973.

[4] Bell, D.E., La Padula, L.J. Secure computer systems: a mathematical model. ESD-TR-73-278, Ⅱ(AD)771 543, Electronic Systems Division, Air Force System Command, Hanscom AFB, Bedford, MA, 1973.

[5] Bell, D.E., La Padula, L.J.Secure computer systems: a refinement of the mathematical foundations. ESD-TR-73-278, Ⅲ(AD)780 528, Electronic Systems Division, Air Force System Command, Hanscom AFB, Bedford, MA, 1974.

[6] Date General Corporation. Managing Security on the Trusted DG/UX™ System (093-701038). Westboro, MA,1994.

[7] Yang, Tao. The Research and design of a secure OP--S_UNIX [Ph.D.Thesis]. Changsha: National University of Defence Technology, 1993 (in Chinese).

附中文参考文献:

[7] 杨涛.一个安全操作系统 S_UNIX 的研究与设计[博士学位论文].长沙:国防科学技术大学,1993.

Design of a Modified BLP Security Model and Its Application to SecLinux*

LIU Wen-qing, QING Si-han, LIU Hai-feng

(*Engineering Research Center for Information Security Technology, Institute of Software, The Chinese Academy of Sciences, Beijing* 100080, *China*)

E-mail: lwq@ercist.iscas.ac.cn

http://www.ercist.iscas.ac.cn

Abstract: In this paper, a MBLP (modified BLP) security model is presented which is PAC (privileged access control) oriented. Some concepts such as role management, domain compartment, limitation of covert channels and defence of viruses, are introduced. MBLP is applied to SecLinux, which is a self-developed secure operating system the authors.

Key words: computer security model; design of secure operating system; PAC (privileged access control); domain compartment

* Received July 3, 2000; accepted December 5, 2000

Supported by the National Natural Science Foundation of China under Grant No.60083007; the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810; the Project for Knowledge Invention of the Chinese Academy of Sciences under Grant No.YC2K5609