ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.1, January 2010, pp.98−106
doi: 10.3724/SP.J.1001.2010.03513

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于Biba和Clark-Wilson策略的混合强制完整性模型*

周洲仪[1,2+], 贺也平[1], 梁洪亮[1]

[1](中国科学院 软件研究所 基础软件国家工程研究中心,北京 100190)

[2](中国科学院 研究生院,北京 100049)

Hybrid Mandatory Integrity Model Composed of Biba and Clark-Wilson Policy

ZHOU Zhou-Yi[1,2+], HE Ye-Ping[1], LIANG Hong-Liang[1]

[1](National Engineering Research Center for Fundamental Software, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: zhouyi04@ios.cn

Zhou ZY, He YP, Liang HL. Hybrid mandatory integrity model composed of Biba and Clark-Wilson policy. *Journal of Software*, 2010,21(1):98−106. http://www.jos.org.cn/1000-9825/3513.htm

Abstract: Commercial application requires protection of integrity policy. Biba model provides a simple multi-level integrity access control scheme but it needs the introduction of trusted subject to ensure the usability. Clark-Wilson model provides a complete integrity protection by means of controlled state transaction, but its entire implementation is hindered by its complication. This paper proposes a model that enforces Biba strict integrity policy as basic access control mechanism, at the same time enforces Biba low-water-mark policy on trusted subjects according to the state in their lifecycle. Clark-Wilson model is used to control and audit subject's state transition and run time adjustment of low-water-mark policy parameters. This paper solves the usability problem introduced by Biba policies and high configuration burden and runtime overload introduced by massive supervising task of Clark-Wilson, while at the same time borrows their merits. This policy composition scheme is proved to be applicable and secure.

Key words: integrity policy; mandatory access control; Biba model; Clark-Wilson model

摘 要: 商业应用需要实施完整性策略保护.Biba 模型提供了一种简洁的多级完整性控制方案,但是需要引入可信主体来保证实施的可用性.而 Clark-Wilson 模型通过可监控的状态转换提供了一种完备的完整性保护,但其复杂性影响了该模型的完整实现.提出的模型以 Biba 严格完整性策略为基础,同时根据可信主体在其生命周期所属的状态实施 Biba 低水标策略.对可信主体在其生命周期发生的状态转换及相应的低水标参数调整,采用 Clark-Wilson 模型来进行监控.在有效解决了 Biba 策略的可用性问题和 Clark-Wilson 模型监控量过大给系统带来的配置和运行负担问题的同时,继承它们的优点.证明了该策略融合方案是可行的、安全的.

关键词: 完整性策略;强制访问控制;Biba 模型;Clark-Wilson 模型

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2007AA010601 (国家高技术研究发展计划(863)); the Defense Pre-Research Project of the "Eleventh Five-Year-Plan" of China (国家"十一五"国防预研项目)

Received 2007-12-16; Revised 2008-06-30; Accepted 2008-10-27

中图法分类号: TP311 文献标识码: A

商业应用需要实施完整性保护.文献[1]指出,完整性保护有 5 大特点:(1) 用户只使用而不开发其运行的程序;(2) 程序员在一台非产品机上开发测试程序;(3) 把程序从开发系统安装到产品系统遵循规定的过程;(4) 必须有监控手段来保证第 3 步所提到的过程的安全性;(5) 系统管理员和审计员必须有访问系统状态和审计记录的权限.为了达到上面的 5 点要求,完整性策略在运行时必须遵循如下原则:(1) 职责分离原则;(2) 功能分离原则;(3) 审计原则;(4) fail-safe原则,即默认拒绝原则[2].Biba完整性模型是最早提出的完整性模型之一,也是业界研究得最透彻的完整性模型[2].该模型有3种变体:(1) 严格完整性策略;(2) 低水标策略;(3) 环策略.严格完整性策略实现Bell-LaPadula模型的对偶模型,一般称Biba模型即为Biba严格完整性策略模型,是一种结构清晰、安全性易验证的策略/模型;低水标策略支持主体标记的动态改变,低水标策略的最大缺陷是,当主体的级别是只降不升的时候,在实际应用中会导致该主体很快就不能访问系统大部分客体;而环策略忽略了间接客体修改,对读访问不加限制,这显然是不可取的.Biba严格完整性策略模型与Bell-LaPadula模型一样,需要引入可信主体来解决可用性的问题.鉴定可信主体的标准是主体对客体的访问违反模型的策略,但是这种访问在系统中是必需的,可以证明该主体引起的信息流动不会违背系统安全性.在最初的Bell-LaPadula模型中,可信主体的权能是不受限制的,它的所有行为都认为是可信的,这显然有违可信主体的定义.所以,强制访问控制多级安全模型的后续研究大都围绕可信主体的权限控制机制展开,比如Bell-LaPadula模型的网络实现以及一些Bell-LaPadula模型的变体[3,4].上述可信主体的研究主要是针对多级机密性策略模型Bell-LaPadula的变体的,但是因为Biba模型是Bell-LaPadula模型的对偶,所以完整性模型同样可以借鉴这些模型的思想,克服这些模型的不足,把Biba模型的可信主体按生命周期划分成不同的状态,而这些状态的确定和在这些状态下的访问控制由Clark-Wilson强制完整性模型来实施.

除Biba模型以外,其他完整性策略模型都有其优缺点.如域型强制实行(domain type enforcement,简称DTE)通过域型访问控制矩阵来实现完整性保护[5],在DTE中主体关联域属性,客体关联型属性.在DTE的变体型强制实行(type enforcement,简称TE)中,主体和客体都关联型属性,著名的SELinux[6]就是采用的TE模型.DTE及TE的特点是访问控制粒度比较细而且不需要可信主体等辅助手段来达到系统的可用,它们的缺点是配置非常繁琐,一个实用系统的策略配置超过一万行,这导致很难发现配置里隐含的安全漏洞.而Clark-Wilson模型[7]是到目前为止理论上最为完备的强制完整性模型,但是很难完整地在整个操作系统上实施模型的思想[8,9].相比较而言,对于完整性策略采用多级安全模型也就是Biba类模型,具有策略描述和配置简洁、安全性易于验证、系统易于维护的特点.

在完整性保护的系统实现方面,Linux Intrusion Detection System(LIDS)通过Linux内核补丁和管理工具实现了Linux下的入侵检测和防护,LIDS有较强的安全性,但是一个实用LIDS的配置是繁琐的,如同SELinux一样,配置上的疏漏会导致保护机制达不到保护策略的预期.AppArmor通过为程序设置安全配置文件等来限制其行为,对于没有对应配置文件的程序,AppArmor是不加限制的,这违背了fail-safe原则.CW-Lite[10]借助程序分析和SELinux机制实现了Clark-Wilson模型的信息过滤的思想,并且给出了对OpenSSH和vsftpd的保护的例子,CW-Lite的实现没有脱离SELinux的框架,不能摆脱SELinux的缺点.Usable Mandatory Integrity Protection (UMIP)[11]采用了类似Biba模型的强制访问控制策略,利用文件的自主访问控制标识作为强制访问控制标识,UMIP能够在一定程度上应对来自网络的威胁,但是因为强制访问控制标识的采用方式及其缺乏对职责隔离等机制的描述,不适合主机系统对登录用户的访问控制.一个好的完整性保护系统从设计思想上要满足文献[1,2]中提到的对完整性定义的 5 个层次要求之一,从具体实现上要保证本文开篇提到的所有 4 个原则.

基于以上分析,本文给出一种基于 Biba 和 Clark-Wilson 策略的混合强制完整性模型.该模型的基本访问控制(占系统大多数的非可信主体)由 Biba 严格完整性策略来实现,同时根据可信主体在其生命周期所属的状态实施 Biba 低水标策略.对可信主体在其生命周期发生的状态转换及相应的低水标参数加以调整,我们采用 Clark-Wilson 模型来进行监控.本文第 1 节给出混合模型的元素和基本访问控制的形式定义.第 2 节给出在

Clark- Wilson 模型控制下的可信主体状态跃迁和特权控制.第 3 节是模型的实现与应用.第 4 节是对相关工作进行总结和比较.

1 混合模型的元素和基本访问控制的形式定义

1.1 混合模型的基本访问控制

模型的基本访问控制由 Biba 严格完整性策略来完成,该模型的基本思想是,通过基于格的访问控制来防止来自低客体的信息流向高客体.

主体集合S: $\mathbb{P}$ *SUBJECT*,包括非可信主体S_{UT}和可信主体S_T.

客体集合O: $\mathbb{P}$ *OBJECT*.

完整性标记集合L: $\mathbb{P}$ *LEVEL*.

访问方式集合A: $\mathbb{P}$ *OPERATION*,包含$\{r,a,e\}$,分别代表只读、只写和执行.

客体完整性标记函数i_o:$O\to L$,该函数把客体映射到相应的完整性标记.

主体完整性标记函数i_s:$S\to L$,该函数把主体映射到其完整性标记.对于非可信主体:$s_1\in S_{UT}$满足$\Xi i_s(s_1)$,即非可信主体的完整性标记在其生命周期内是不能浮动的(符号Ξ符合Z形式规范语言表述,表示该模式是操作不变的).对于可信主体:$s_2\in S_T$满足$\Delta i_s(s_2)$.即可信主体的完整性标记在其生命周期内是动态调整的(符号Δ符合Z形式规范语言表述,表示该模式是操作可变的).

非可信主体的访问控制规则:

(1) $s\in S_{UT}$可以只读$o\in O$当且仅当$i_s(s)\prec i_o(o)$;

(2) $s\in S$可以只写$o\in O$当且仅当$i_o(o)\prec i_s(s)$;

(3) $s_1\in S$可以执行$s_2\in S$当且仅当$i_s(s_2)\prec i_s(s_1)$,

其中第 2 条、第 3 条规则对可信主体和非可信主体都是适用的,即主体只能只写(追加写)完整性级别为其所支配的客体,主体只能执行完整性级别为其所支配的主体.

根据以上规则,我们有如下完整性定理:

定理 1. 如果存在一条从客体$o_1\in O$到客体$o_{n+1}\in O$的信息流动路径,那么如果只有非可信主体参与该流动过程,那么本文模型的实施可以保证$i_o(o_{n+1})\prec i_o(o_1)$.

证明:假设存在一条从客体o_1到客体o_{n+1}的信息流动路径,则对于所有的k,$1\le k\le n$存在主体序列$s_1,\ldots,s_n$,满足$s_k \underline{r} o_k$和$s_k \underline{a} o_{k+1}$.因为只有非可信主体参与该流动过程,所以根据模型的访问规则和非可信主体完整性标记的生命周期不变性,有$i_o(o_{k+1})\prec i_o(o_k)$,定理由归纳法得证. □

定理 1 表明,只有非可信主体参与的信息流动不会把低级别客体的信息写入高级别的客体,从而保证了模型的完整性.但是,如同多级完整性模型的对偶多级机密性模型一样,只有非可信主体参与的系统是不可用的,模型必须按照最小特权原则引入可信主体机制.

模型的可信主体机制采用 Biba 低水标策略,不对所有主体采用低水标策略的原因是,低水标策略的完整性标记动态调整很快会使被调整的主体不能写大部分客体,对于系统中的可信主体来说,我们可以采用 Clark-Wilson 模型的思想来对其低水标参数重新调整,若对所有主体实施 Clark-Wilson 模型,则监控代价太高.

1.2 混合模型的可信主体访问控制

系统可信主体的访问控制在其特权状态不变时,遵从 Biba 低水标策略:

(1) 如果$s\in S_T$只读$o\in O$,则$i^*(s)=\min(i(s),i(o))$,这里,$i^*(s)$是主体在读之后的完整性标记;

(2) $s\in S$可以只写$o\in O$当且仅当$i_o(o)\prec i_s(s)$;

(3) $s_1\in S$可以执行$s_2\in S$当且仅当$i_s(s_2)\prec i_s(s_1)$.

定理 2. 如果存在一条从客体$o_1\in O$到客体$o_{n+1}\in O$的信息流动路径,那么如果所有参与信息流动过程的可信主体保持其特权状态不变,那么本文模型的实施可以保证,$i_o(o_{n+1})\prec i_o(o_1)$.

证明:假设存在一条从客体o_1到客体o_{n+1}的信息流动路径,则对于所有的k,$1\le k\le n$存在主体序列$s_1,\ldots,s_n$,满足s_k r o_k和s_k a o_{k+1}.因为所有参与该流动过程的主体保持其特权状态不变,根据规则 2,主体s_k的读后完整性标记被o_k的完整性标记所支配,而根据规则 1,$i_o(o_{k+1})\prec i_s(s_k)$,所以,根据模型的访问规则和非可信主体完整性标记的生命周期不变性有$i_o(o_{k+1})\prec i_o(o_k)$,定理由归纳法和定理 1 的结论得证. □

如前所述,采用低水标策略的主体标记会逐渐降低标记,最后变得不可用.Biba 低水标策略没有考虑到可信主体的低信息清理和经过验证后的低信息写入情况,例如在财务系统中,记帐信息写入信息会定期将缓冲区内的低完整性信息清除;另一方面,经过给定管理员共同认证的输入信息实际上已经是高级别信息.因此,本模型允许可信主体在一定条件下进行安全的状态转换,把完整性标记调整到可用的级别,并保证这个转换(及对应的调整)不会造成违背系统安全目标的信息流动.这种转换的发生和监控是由 Clark-Wilson 模型来完成的.

1.3 用于监控可信主体特权状态转换的Clark-Wilson模型的元素

- *UDIs*(非受控数据项集合):包括用户输入等非受控信息;
- *CDIs*(受控数据项集合):在本监控模块中,*CDIs* 由两个元素组成的集合:

Log: ℙ *LOG*(*LOG* 由第 2 节中定义 2 来定义)

privState:$S_T\rightarrow$*privStates*

第 1 个元素由审计记录组成,Clark-Wilson 模型默认地把所有的审计信息看成一个受控数据项,每个 *TP*(转换过程)可以追加审计信息,但是任何 *TP* 都不能篡改审计信息.第 2 个元素是可信主体与特权状态之间的对应函数.

可信主体的生命周期状态转换与特权状态转换之间的关系如图 1 所示.

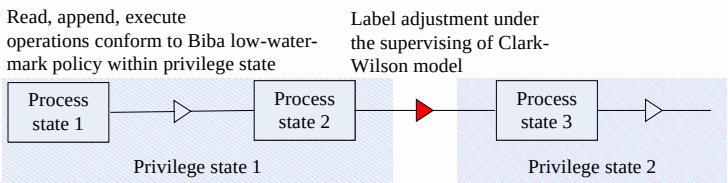


Fig.1 Process status and privilege status transaction of trusted subject

图 1 可信进程的进程状态转换与特权状态转换

图1中,系统中的可信主体在特权状态1下遵从Biba低水标策略动态进行完整性标记调整(同时完成进程状态跃迁).当出现主体不满足系统发出的读客体请求时($i_o(o)!\prec i_s(s)$),系统将在Clark-Wilson模型的监控下按照最小特权原则进行特权状态调整,尽可能地在保证安全的前提下满足读客体请求,本文将在第 2 节作详细论述.另外,从图 1 可以看出,在同一特权状态下,系统中的可信主体是遵从Biba低水标策略的.

- *TPs*(转换过程集合):

在本模块中,*TPs* 由若干转换过程组成,这里给出最重要的两个:

TP_{log}:*Log*⇒*Log*′

$TP_{privstate}$:*privState*⇒*privState*′

第 1 个转换过程是审计记录改变过程,因为系统行为,系统的审计记录将作相应的改变.第 2 个转换过程是特权状态映射函数的改变,模型通过审计和监控将动态影响特权状态映射函数,也即实现可信主体的特权状态转换.为了实现Clark-Wilson模型的职责分离原则,$TP_{privstate}$由 3 个子转换过程组成:$TP_{privstate1}$,$TP_{privstate2}$和$TP_{privstate3}$,具体在第 2 节加以论述.

- *IVP*(完整性验证过程)

本模块的完整性验证过程由

1) 本模型审计信息 *Log* 的完整性用前向完整性验证的方法加以验证,具体在第 2 节加以论述;

2) 对特权状态映射函数的验证:*conform*(*privState*,*Log*),也即审计记录表明当前的特权状态映射是不会破

坏完整性的.

2 Clark-Wilson 模型控制下的可信主体状态跃迁和特权控制

文献[4]中提到的可信主体的特权状态确定的主要依据是对应用程序的分析和程序的当前代码执行位置.而本模型中可信主体的特权状态则是通过对访问请求的分析和对审计信息的分析得到的综合结果,其含义概括而言是模型根据访问请求得到可信主体要满足该访问请求的最低调整指标,再根据审计记录分析出该主体当前能够在不破坏完整性的前提下能够调节到的最高调整指标,如果后者支配前者,则主体的完整性标记调整为后者,主体自然进入下一个特权状态(这里的特权状态只是一个 Biba 低水标阶段的表示,并无如同文献[4]等的特权状态不变量),否则,在若干管理员共同参与下将可信主体的完整性标记调整为能够满足该访问请求的最低指标,主体自然进入下一个特权状态,如果以上管理员之一拒绝调整,则主体保持当前特权状态不变(即不对主体完整性标记作调整).

本模型的审计子系统的形式定义借鉴了文献[12]的审计模型的思想,除特别说明以外,本文以下使用的符号与注记与文献[12]相同.

从本模型的审计子系统的角度看来,系统可以用一个 4 元组$(C,States,s_0,T)$表示(因为系统状态类型符号S在本模型中已用来表示主体类,所以这里以$States$作替换.基于类似的原因,有$O\to LOG,o\to\delta$).这里,C是使系统发生改变的事件的集合,$States$是系统状态的集合,s_0是起始系统状态,T是系统状态改变映射集合.

定义 1. 设N是一列非负整数.系统状态历史是一个函数$\Pi:N\to C\times States$,$\Pi(0)$的第 2 个元素是s_0,并且满足$\forall n\in N[[\Pi(n)=(c,s)$ and $\Pi(n+1)=(c^*,s^*)]\to s^*\in T(c,s)]$.系统子状态相关历史是一个函数$\pi:N\to C_I\times\Sigma$满足$\forall n\in N[[\Pi(n)=(c,s)\to\pi(n)=(c,\sigma)]$.其中,$\Sigma$是系统相关状态子空间,而系统相关子状态$\sigma$包含的信息是系统状态$s$包含的信息的一个子集,即系统状态中模型关心的那些内容.引入系统相关子状态空间的原因是系统状态包含的信息太多,审计系统在审计分析和抽取过程中只关注某些重要的部分.

在本模型中,系统相关子状态空间Σ包含的元素类型是系统状态中与完整性相关的元素类型的集合,例如由 read 系统调用导致的带完整性级别的可信主体信息流入、由 write 系统调用导致的带完整性级别的可信主体信息流出、由于各可信主体专有的各级缓冲区(主体与系统共享缓冲区的信息交流可视作主体的读或写访问)的存在而导致的带完整性级别的信息驻留等.

定理 3. 本模型中完整性相关部分Σ是自包含的(系统相关子空间是自包含的表明可以仅仅通过审计该子空间实现系统相关子状态推导).

证明:根据文献[12]的定义,一个系统相关空间是自包含的,如果$\forall i[T_i(State_{i-1})=State_i\to\exists\tau_i[\tau_i(\sigma_{i-1})=\sigma_i]]$.在本模型中,$\Sigma$包含了由各可信主体所涉及的所有信息流动信息和带完整性级别的信息驻留,而$\tau_i:C_I\times\Sigma\to\Sigma$的第 1 个参数提供了某主体的访问操作,那么我们可以根据这个访问记录下这次访问导致的信息流动,并且可以从此次信息流动过程和上一状态的信息驻留情况得到以上操作所涉及主体的下一状态的信息驻留情况. □

定义 2. 本模型中,系统状态历史表示为$LOG=\{\delta_0,\delta_1,\ldots,\delta_m\}$,而以$\sigma_0,\sigma_1,\ldots$表示系统状态的完整性相关历史.

定义 3. 设$Log_i=\{\delta_k|k\le i\}$,本模型审计抽取函数定义为$\gamma$ and $\alpha:\mathbf{P}\,LOG\to\Sigma$,满足$\gamma$ and $\alpha(Log_i)=\sigma_i$.可信主体当前驻留最低完整性标记函数定义为$LowestLevel:\Sigma\times S\to L$,该函数的作用是通过特定操作系统审计分析方法总结出当前驻留在给定可信主体上的具有最低完整性的信息的完整性级别**.如果可信主体无当前驻留信息,则我们记$LowestLevel(\sigma_i,s)=systemhigh$,即系统最高完整性标记.根据定理 3,因为本模型中完整性相关部分Σ是自包含的,所以可只审计完整性相关信息也能总结出给定可信主体的最低驻留信息级别.但是,在实际系统中,对除完整性相关信息以外的其他信息的审计是必要的,这也是本模型的默认事实.

** Biba标记由等级元素和范畴元素组成,其完整性标记级别之间的比较是在格的基础上进行的.这里为了论述方便,在不引起歧义的情况下,将最低完整性信息级别的最大下界描述成具有最低完整性信息的完整性级别,即抽象出一个具有最低完整性级别的最大下界的信息,下同.

系统在以下两种情况下试图触发可信进程特权状态跃迁:

(1) $s\in S_T$请求写$o\in O$并且$i_o(o)!\prec i_s(s)$,此时,我们记特权状态跃迁请求级别$AccessRequestLevel=i_o(o)$.

(2) $s_1\in S$请求执行$s_2\in S$并且$i_s(s_2)!\prec i_s(s_1)$,此时,我们记特权状态跃迁请求级别$AccessRequestLevel=i_s(s_2)$.

可见,可信进程特权状态跃迁触发条件是进程当前完整性级别未高到能够完成系统访问请求的程度.

可信进程特权状态跃迁规则:

$$PrivStateTrans:S_T\times privStates\times \mathbb{P}\,LOG\times L\rightarrow privState\times \mathbb{P}\,LOG: \tag{1}$$

$PrivStateTrans(s,privState_j,Log_j,AccessRequestLevel)=$

if $AccessRequestLevel\prec LowestLevel(\gamma \text{ and } \alpha(Log_j),s)$

then begin

$(privState_{j+1},Log_{j+1})$

$\{StartLevel(privState_{j+1}(s))=LowestLevel(\gamma \text{ and } \alpha(Log_j),s) \text{ and } \forall s'\neq s\cdot\Xi privState(s')\}$

end

else if $TransPrivStateByForce(s,privState_j,Log_j,AccessRequestLevel)$==true

then begin

$(privState_{j+1},Log_{j+1})\{StartLevel(privState_{j+1}(s))=AccessRequestLevel \text{ and } \forall s'\neq s\cdot\Xi privState(s')\}$

end

else begin $(privState_j,Log_{j+1})$ **end**

公式(1)的第 1 个条件分支表明,可信进程特权状态发生自动跃迁并且跃迁后的特权状态的起始完整性标记是审计分析函数分析出来的跃迁前主体的最低驻留信息完整性标记,在第 1 个条件分支下完成的可信主体特权状态跃迁无论如何也不会造成对 Biba 模型意义上的完整性的破坏;在第 2 个条件分支的第 1 个分支表明,可信进程特权状态发生强制跃迁并且跃迁后的特权状态的起始完整性标记是触发此次特权状态跃迁的请求级别,第 2 个条件分支的第 1 个分支得以满足的判断函数是 *TransPrivStateByForce*,如果该判断函数返回真,则表明系统在 Clark-Wilson 模型规则监控下完成了对 *UDI* 的处理和对 *CDI*:*privState*,*Log* 的转变.第 2 个条件分支的第 2 个分支表明,可信进程特权状态不发生跃迁,触发此次请求的操作无法完成.

上节已经给出了监控可信主体特权状态转换的 Clark-Wilson 子模型的基本元素,现在描述与 Clark-Wilson 子模型 9 条规则对应的 4 组可信主体特权状态转换相关策略.

*CR*1:

在混合模型的Clark-Wilson子模型中,首先要确保审计记录的完整性,而使用前向完整性验证[13]的方法可以实现这一要求.

审计函数定义如下:$log\_fn_j(\delta_i)=(\delta_i,FIMAC_j(\delta_i))$,这里,$FIMAC_j(\delta_i)$是添加到系统状态审计记录后的前向认证值.本模型的前向认证对文献[13]进行了改进,在文献[13]中,$FIMAC_j$的认证钥由$FIMAC_{j-1}$的认证钥经由单向函数f生成,如果攻击者窃取了任一认证钥,虽然其不能伪造前面的审计记录,但仍可以伪造其后的审计记录.本模型的改进如下:$Key(FIMAC_j)=f(Key(FIMAC_w))$,这里,$w=hash(j,\prod_{k<j}|\,\delta_k\,)$,Hash函数的值分布在 0 和$j-1$ 之间.这样,伪造者即使截获了当前审计认证钥,因为其很难得到历史审计认证钥,所以很难伪造任何有意义的审计信息.此外,审计定期更换新的$FIMAC_0$,进一步增加了伪造审计信息的难度.审计记录验证过程:

$$logvalidation(\delta_i,j,x)\xleftrightarrow{\text{def}}x==FIMAC_j(\delta_i) \tag{2}$$

CDIs 的另一个元素是可信主体与特权状态之间的对应函数 *privState*,其验证过程是 *conform*(*privState*, *Log*),即根据审计信息来判断当前可信主体的特权状态分配是否合理.以财务系统为例,该函数将验证如果记帐信息写进程高于记帐信息的完整性级别,则要么审计历史,表明该进程中已无低信息;要么该进程的高完整性级别是在系统自身、系统管理员和安全管理员的共同批准下调高的.

*CR*2-*CR*3-*CR*4-*CR*5-*ER*1-*ER*2:

系统审计信息的改变由并且只能由内核审计模块自动完成,TP_{log}:$Log\Rightarrow Log'$的可靠性是由内核编码来保证

的,TP_{log}对应的用户是系统自身.

$TP_{privstate1}$是可信主体特权状态转换的第 1 阶段,相当于公式(1)的第 1 个判断语句的判断和控制跳转过程.系统通过对审计信息的分析,判断是否可信主体中还存在完整性级别低于访问请求要求的完整性级别的信息:如是,则把控制交由$TP_{privstate2}$,即公式(1)的第 2 个条件分支;否则按公式(1)的第 1 个条件分支的语句改变*privState*.模型把$TP_{privstate1}$和系统默认用户、特权状态映射函数*privState*组合成一个三元关系(系统自身,$TP_{privstate1}$,*privState*),表明该转换涉及*CDI*:*privState*且该转换的执行是以系统默认用户的名义执行的.在类Unix系统中,系统自身默认的用户是系统的第1个进程所对应的用户,其uid为 0.$TP_{privstate1}$的触发和执行是非交互的、自动的.

$TP_{privstate2}$,$TP_{privstate3}$是可信主体特权状态转换的第 2 阶段,此阶段可以是交互的、非自动的.模型定义两个三元组(系统管理员,$TP_{privstate2}$,*privState*)和(安全管理员,$TP_{privstate3}$,*privState*).$TP_{privstate1}$把控制交给$TP_{privstate2}$后,系统管理员总结出低完整性信息存在的位置,并判断是否应该交由安全管理员作进一步判断:若否,则按公式(1)的第 2 个条件分支的第 2 个分支的语句保持可信主体当前的特权状态不变;若是,则将控制交由$TP_{privstate3}$.在$TP_{privstate3}$中进一步由安全管理员判断引发可信主体特权状态转换的操作是否会破坏被写客体的完整性:若是,则按公式(1)的第 2 个条件分支的第 2 个分支的语句保持可信主体当前的特权状态不变;否则,按公式(1)的第 2 个条件分支的第 1 个分支的语句进行特权状态调整.$TP_{privstate2}$,$TP_{privstate3}$体现了职责分离的原则,比如在财务系统中,当外来的记帐信息欲进入高完整级别的记帐文件时,系统管理员和安全管理员共同保证记帐文件变更的完整性.事实上,如果需要更多人员参与职责分离,则$TP_{privstate}$可以根据具体应用变更或扩充.

*ER*3:

TP_{log}:和$TP_{privstate1}$的用户是系统默认用户,他们的可靠性由内核本身来保证.而$TP_{privstate2}$和$TP_{privstate3}$的用户将实时地被认证.以财务系统为例,当外来的记帐信息欲进入高完整级别的记帐文件时,系统可实时请求系统管理员和安全管理员等输入密码或插入智能卡或输入指纹信息等.

*ER*4:

本模型中 *TPs* 和 *CDIs* 是固定的,与 *TP* 有关的元素由编码来实现.

3 模型的实现与应用

模型在 FreeBSD-6.0 的基础上进行了实现.FreeBSD 的 MAC 框架为我们的工作提供了一个很好的基础.从 FreeBSD5.0 开始,MAC 框架作为一个子模块正式进入 FreeBSD 发行版,为 FreeBSD 操作系统提供了一个符合 posix.1e 草案的访问控制基本框架.在 MAC 框架已有的工作中,mac_lomac 策略模块实现了初步的 Biba 模型低水标策略.为了实现模型的思想,本文对 mac_lomac 策略模块进行了完善.例如,原有策略模块中高级别的进程在从套接字获取低级别的数据包未对进程的标记进行动态调整,而本文按照低水标策略对读取套接字进程的标记进行了动态调整.另外,本文通过动态 Hash 表维护一个可信进程清单.本文的 mac_lomac 模块不对非可信进程的标记进行动态调整,以符合模型的要求.模型之所以不对所有进程实施低水标策略的原因在第 1.1 节已有论述.

对于系统中的可信进程,mac_lomac 按照低水标策略对其标记进行动态调整.而当可信进程的标记不能满足实际应用场景的需要时,系统根据 Clark-Wilson 模型对其进行标记升级.升级分为两种情况:一是比较简单的情形,由多个用户共同干预来升级.本文通过修改 bash,利用 ncurse 库提供一个多用户输入用户名和密码的界面来完成这项操作;另外一种是比较复杂的情形,即基于审计信息的自动标签升级.以 openssh 为例,文献[14]利用特权隔离防止对 openssh 的网络攻击,文献[14]的工作已成为 openssh 发布版的一个标准选项:UsePrivilege Separation[default yes].文献[14]对本文的工作有很大的借鉴意义,但是因为 openssh 作为系统的一部分,其标记变化受系统总体策略制约,文献[14]的改进在 Biba 类策略下将不可用,本文不使用此机制.我们在 openssh-4.6p1 的基础上对来自外部的数据包按照 SSH 的不同阶段对其解密的内容进行审计,在需要标记提升的代码(例如打开伪终端操作 openpty 等)前插入标记提升系统调用,内核根据审计信息和系统调用上下文拒绝或进行相应的

标记提升操作.

最后,我们利用 lmbench 对系统带来的额外开销进行了分析,结果见表 1(测试机器配置为 Pentium IV 3.0G, 1MB L2 cache,512DDR2 Memory,80G 7200 转硬盘).

Table 1 System overhead (Unit: ms)

表 1 系统的开销测试 (单位:ms)

	Read system call	Write system call	Open/Close system call	10 select calls on TCP	Process fork	Process fork+ exec
Unlabeled system	0.66	0.63	5.19	0.97	228	889.5
This system	0.88	0.82	9.1	1.27	354	1260.6

其他与系统调用关系不大的操作,如I/O和内存读写等没有额外开销.两者综合,通过loadrunner对系统上运行的 apache 进行小页面压力测试、访问控制及标记机制给系统带来的平均额外开销为 23%左右.

本文的系统作为中科方德安全操作系统 NFSARK 的一部分,成功地布署和运行在无锡旅游网和中科方德邮件系统等节点上,保护了这些节点的关键数据,如系统配置文件、密钥、数据库文件等的完整性,实现了最少的运行时人工干预.

4 结束语

商业和工业应用对于可信系统最关注的是数据的内在和外在一致性,也即完整性.为了达到这一目标,可信系统必须实施完整性策略来阻止非授权用户对保护对象的修改行为,阻止授权用户对保护对象的不恰当的修改行为.学术界和工业界提出了许多用于完整性保护的策略,例如 Biba 系列策略、Clark-Wilson 策略、Lipner 策略和 TE,DTE 策略等.

比较而言,Biba系列策略模型属于格模型的范畴,其突出优势在于主客体标记机制和策略简单、明确,易于实施和验证.但是,现有的Biba系列策略都存在可用性问题,例如,低水标策略和Biba严格策略的动态实施[15]都会随着主体的长时间运行失去可调节性.而Clark-Wilson模型是最为完备的完整性模型,但很难实施于整个系统.

本文分析了 Biba 模型严格完整性策略、Biba 模型低水标策略和 Clark-Wilson 模型的特点,提出了一种基于以上 3 种策略的混合模型.对于非可信主体,本文采用 Biba 严格完整性策略加以控制,其完整性标记在整个生命周期内是不变的;对于可信主体,本文采用 Biba 低水标策略来控制其在特权状态内的访问和标记的变化,用 Clark-Wilson 模型来控制其特权状态之间标记的变化.与其他完整性保护系统相比,本文的系统在确保遵循完整性原则的基础上,最大限度地提升了系统的可用性.此外,本文基于审计的特权状态转换的思路对于多级机密性安全策略模型的设计与实现也有非常好的借鉴意义.

致谢 在此,我们向对本文工作给予支持和建议的审稿老师、贺也平研究员组织的讨论班上的同学表示感谢.

References:

[1] Lipner SB. Non-Discretionary controls for commercial applications. In: Proc. of the 1982 Symp. on Privacy and Security. Oakland, 1982. 2−10. http://www.computer.org/portal/web/csdl/doi/10.1109/SP.1982.10022

[2] Bishop M. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.

[3] He JB, Qing SH, Wang C. Formal safety analysis of a class of multilevel security models. Chinese Journal of Computers, 2006, 29(8):1468−1479 (in Chinese with English abstract). http://cjc.ict.ac.cn/quanwenjiansuo/2006-08/hjb.zip

[4] Liang B, Liu H, Shi WC, Wu YJ. Enforcing the principle of least privilege with a state-based privilege control model. In: Bao F, Pang H, Zhou JY, eds. Proc. of the 1st Information Security Practice and Experience Conf. Singapore: Springer-Verlag, 2005. 109−120.

[5] Badger L, Sterne DF, Sherman DL, Walker KM, Haghighat SA. Practical domain and type enforcement for UNIX. In: Proc. of the '95 IEEE Symp. on Security and Privacy. 1995. 66−77. http://www.computer.org/portal/web/csdl/doi/10.1109/SECPRI.1995.398923

[6] Smalley SD. Configuring the SELinux policy. Technical Report, #02-007, NAI Labs., 2002. http://www.nsa.gov/seLinux/papers/policy2-abs.cfm

[7] Clark D, Wilson D. A comparison of commercial and military security policies. In: Proc. of the '87 IEEE Symp. on Security and Privacy. 1987. 184−194. http://www.computer.org/portal/web/csdl/doi/10.1109/SP.1987.10001

[8] Qing SH, Wen HZ, Lei H, Wang J. A secure monitoring model based on the Clark-Wilson integrity policies. Journal of Software, 2004,15(8):1124−1132 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1124.htm

[9] Abrames MD, Joyce MV. Trusted system concepts. Computers and Security, 1995,14(1):45−56.

[10] Shankar U, Jaeger T, Sailer R. Toward automated information-flow integrity verification for security-critical applications. In: Proc. of the 2006 ISOC Networked and Distributed Systems Security Symposium. 2006. http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/automated_information_flow_verification.pdf

[11] Li NH, Mao ZQ, Chen H. Usable mandatory integrity protection for operating systems. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. 2007. 164−178. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4223222

[12] Bishop M. A model of security monitoring. In: Proc. of the IEEE 5th Annual Computer Security Applications Conf. New York: IEEE Computer Society Press, 1989. 46−52. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=81024

[13] Bellare M, Yee BS. Forward integrity for secure audit logs. Technical Report, UC at San Diego: Department of Computer Science and Engineering, 1997. ftp://www.cs.ucsd.edu/pub/bsy/pub/fi.ps

[14] Provos N, Friedl M, Honeyman P. Preventing privilege escalation. In: Proc. of the 12th USENIX Security Symp. Washington, 2003. 231−241. http://www.usenix.org/events/sec03/tech/provos_et_al.html

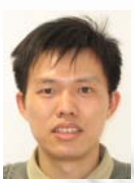
[15] Zhang XF, Sun YF. Dynamic enforcement of the strict integrity policy in Biba's model. Journal of Computer Research and Development, 2005,42(5):746−754 (in Chinese with English abstract). http://crad.ict.ac.cn:81/CRAD/ePublish/Downloads/DownloadFile.asp?pno=178

附中文参考文献:

[3] 何建波,卿斯汉,王超.对一类多级安全模型安全性的形式化分析.计算机学报,2006,29(8):1468−1479. http://cjc.ict.ac.cn/quanwenjiansuo/2006-08/hjb.zip

[8] 卿斯汉,温红子,雷浩,王建.基于 Clark-Wilson 完整性策略的安全监视模型.软件学报,2004,15(8):1124−1132. http://www.jos.org.cn/1000-9825/15/1124.htm

[15] 张相锋,孙玉芳.Biba模型中严格完整性政策的动态实施.计算机研究与发展,2005,42(5):746−754. http://crad.ict.ac.cn:81/CRAD/ePublish/Download/DownloadFile.asp?pno=178



周洲仪(1975－),男,湖南衡东人,博士,主要研究领域为系统软件安全技术,编译技术.

贺也平(1962－),男,博士,研究员,博士生导师,主要研究领域为系统软件安全技术,安全协议的设计与分析.

梁洪亮(1972－),男,博士,副研究员,主要研究领域为系统软件,信息安全.