# 基于可变标签的访问控制策略设计与实现

李大明 曹万华 张 焕
(武汉数字工程研究所 武汉 430074)

**摘 要** 仅提供了自主访问控制级安全防护能力的Windows操作系统的安全性受到用户广泛关注,而作为一项重要的信息安全技术,强制访问控制能够有效实现操作系统安全加固。访问控制策略的选择与设计是成功实施强制访问控制的关键。针对安全项目的需要,分析了结合经典访问控制模型BLP与Biba的优势,提出了依据进程可信度动态调整的可变标签访问控制策略,解决了因BLP与Biba模型的简单叠加而导致的系统可用性问题,最终实现了对进程访问行为进行控制的简单原型系统。实验表明,可变标签访问控制策略的引入在对操作系统安全加固的基础上显著提高了系统的可用性。

**关键词** BLP,Biba,安全标签,标签调整,进程可信度
**中图法分类号** TP316.7 **文献标识码** A

## New Label Alterable Access Control Policy

LI Da-ming CAO Wan-hua ZHANG Huan
(Wuhan Digital Engineering Institute, Wuhan 430074, China)

**Abstract** The security of Windows operating system which only provides discretional access control (DAC) capability has riveted far and wide attention. As an important information security technology, mandatory access control (MAC) can effectively enhance security of system, and the design of access control policy plays a key role in successful implementation of MAC. In order to satisfy the needs for secure projects in Windows operating system ultimately, combining advantages of classical access control models BLP and Biba, a new access control policy which adjusts security label of subjects based on its credibility was presented to solve poor usability caused by superposition of BLP and Biba. And finally the prototypal system based on access from process to file shows that the usability and security of system are improved effectively.

**Keywords** BLP, Biba, Security label, Label adjusting, Process credit

## 1 引言

Windows是目前最流行,也是经常遭受入侵与攻击的计算机操作系统。据市场调研机构Net Application发布的2011年6月全球操作系统市场份额显示:Windows系列操作系统以88.69%的绝对优势全球第一[1],在我国,Windows操作系统使用率达到了惊人的98.58%[2],而每年针对Windows操作系统的攻击事件层出不穷。对仅提供了自主访问控制级安全防护能力的Windows操作系统进行旨在提高信息机密性、完整性以及可用性的改进迫在眉睫。作为一项重要的信息安全技术,强制访问控制(MAC,Mandatory Access Control)采用特定访问控制策略来协调对系统资源的访问,并限制信息的不安全流动,抵御来自系统内、外的攻击,维护系统的安全与稳定。

访问控制策略的选择与设计是成功实施强制访问控制的关键,经典的访问控制策略包括关注受控信息机密性的BLP模型和对受控信息进行完整性约束的Biba模型。BLP模型是由Dave Bell和Len LaPadula提出的模拟军事安全策略的多级安全模型,它为系统实体分配机密性等级;Biba模型是仿照BLP模型构造的,定义了每个实体的完整性级别和完整性级别间的偏序关系。BLP模型与Biba模型的不同之处在于BLP模型注重保护信息的机密性,防止信息非授权泄露,而Biba则注重信息的可信度,防止信息非授权篡改。

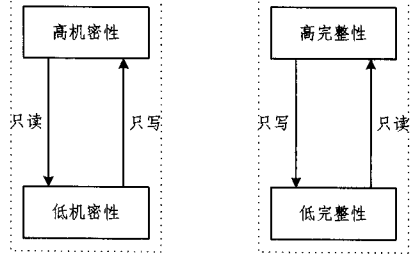


图1 BLP与Biba模型对信息流的控制

到稿日期:2012-02-14 返修日期:2012-07-29 本文受国防"十二五"预研计划(4010105010103,62101050101,513150802),船舶基金(09J3.4.1)资助。

李大明(1986—),男,硕士生,主要研究方向为操作系统内核安全,E-mail:hustldm@163.com;曹万华(1966—),男,博士生导师,主要研究方向为计算机软件与理论。

然而，BLP 模型与 Biba 最根本的区别是：BLP 模型依据机密性等级实施“向下读，向上写”，而 Biba 则根据信息完整度实施“向下写，向上读”，如图 1 所示。现实中，具有较高机密性要求的信息往往也具有较高完整性要求，这种机密性与完整性一致的情形是比较普遍的。如果简单地将 BLP 模型与 Biba 模型进行叠加，会导致系统的可用性显著下降[3]，因此在实际中要么实现 BLP 模型，要么实现 Biba 模型。

本文讨论了 BLP 与 Biba 模型，提出了依据进程可信度动态调整的可变标签访问控制策略，实现了对进程访问行为进行控制的原型系统。

## 2 相关技术

### 2.1 混合访问控制策略

在不影响系统可用性的前提下有机融合 BLP 模型与 Biba 模型的新型访问控制策略的研究，是实现操作系统安全加固的重要手段与途径。根据主、客体安全级关系，主体对客体的访问在 BLP 策略与 Biba 策略下的授权规则如表 1 所列。

表 1 BLP 与 Biba 模型授权规则

| 主体相对客体安全级 | | BLP | Biba |
|---|---|---|---|
| 机密性 | 完整性 | | |
| 高 | 高 | 可读 | 可写 |
| 高 | 低 | 只读 | 只读 |
| 低 | 高 | 只写 | 只写 |
| 低 | 低 | 可写 | 可读 |

由表 1 可知，当主体相对客体机密性属性与完整性属性一致时，在不同的访问控制策略下将得到截然不同的授权结果。目前针对 BLP 模型与 Biba 模型结合的研究包括以下 3 类：

简单混合模型，指将多个访问控制策略模型进行堆叠，各安全策略单独实现。Linux 安全框架（LSM，Linux Security Model）也采用这种链式或栈式方法，将多个访问控制策略模型串联起来形成策略栈，主体对客体的访问请求需要依次经过策略栈的检查。简单混合模型的优势是各访问控制策略模型独立开发、按需加载、自由组合，但其无法实现真正的结合，并且访问请求需要多次递归判断，对系统性能的影响不可控。

复杂格模型。BLP 模型中基于主、客体机密性可以构成一种格理论模型，Biba 模型中基于主、客体完整性也可以构成一种格理论模型。因此对 BLP 和 Biba 格模型的自然延伸就是根据机密性和完整性属性组成二元组来构造格理论模型。复杂格模型的优点是简洁直观，安全性容易证明，但是其忽略了一个重要背景：复杂格模型要求主、客体的敏感标记同时满足相同的偏序关系，无法应用于不一致的情形[4]，当主体 $S$ 的机密性高于客体 $O$，而 $S$ 的完整性低于客体 $O$ 时，复杂格模型无能为力。

动态统一模型。根据主体相对于客体的安全等级划分为 4 类：高机密性高完整性、高机密性低完整性、低机密性高完整性和低机密性低完整性。对高（低）机密性和高（低）完整性严格执行 BLP 和 Biba 模型则导致矛盾，在这种情况下，要么根据所要保护信息的特点选择执行 BLP 策略或者 Biba 策略，要么让实体的敏感标签具有一定的波动范围，在保证系统安全与可用性[5]的前提下实现机密性与完整性的统一。

此外，李益发提出的可信主体的概念对解决 BLP 和 Biba 无法使机密性和完整性兼顾的问题进行了有益的尝试[6]，但对可信主体本身没有给出明确的证明；黄强等提出的基于可信计算的保密性和完整性统一安全策略模型[7]也存在类似的问题。这些模型无法成功的原因是它们都试图用一种等级划分方法去衡量保密性和完整性这两个截然不同的属性，在 BLP 模型中维护完整性和在 Biba 模型中维护机密性天生就存在缺陷。本文提出了结合 BLP 和 Biba 模型优点、安全标签可动态调整[8]、具有一定容忍度的新型访问控制策略。

### 2.2 进程可信度

程序是为实现某个功能而编写的，具备较强的专用性与目的性，进程是程序的一次动态执行过程，预设功能决定了其在执行过程中对系统资源的访问与操作具备固定的模式[9]。如 Ms Paint 是 Windows 自带的画图程序，功能包括图片的编辑与保存，因此进程 mspaint 运行的正常行为包括打开、编辑与保存图片。如果进程 mspaint 调用打印机程序或其它可执行文件，导致其脱离了程序 Ms Paint 预设功能所许可的正常轨迹而表现出行为异常。

调用系统服务分配表（SSDT，System Service Distribution Table）[10]而产生的 Native API 序列监控能够将这种偏离正常轨迹的异常行为有效检测出来，如依据 API 调用频率和相邻 API 对出现概率[11]来提取进程行为特征：进程运行正常时，进程行为状态值稳定地趋近设定值 1；系统遭受攻击时，进程行为状态值急剧下降并出现剧烈波动。本文定义进程行为状态值的稳定程度为进程可信度，其为主体安全标签的动态调整提供了直接依据。

在复杂环境下，对进程运行状态进行监控可得到如图 2 所示的进程行为状态值曲线。

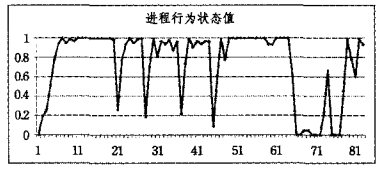


图 2 典型进程行为状态值

进程可信度与进程行为状态值的波动情况直接相关。由图 2 可知，进程行为状态值波动越频繁，如 API 数为 21 到 49 时，则进程运行异常，其可信度越低；进程行为状态值越稳定，如 API 数为 49 到 63 时，则进程运行正常，其可信度也越高。

## 3 系统详细设计

### 3.1 安全标签的设计与分析

传统访问控制策略通过划分安全等级为主、客体分配固定安全标签，主体对系统资源的访问能力由系统管理员预先分配与修改。本文设计的安全标签是由机密性属性与完整性属性构成的二维偏序关系，客体依然采用固定安全标签，而主体安全标签则采用由最高值与最低值界定的可变区间。如图 3 所示，平面坐标系的横轴代表完整性属性，纵轴代表机密性属性，客体依据其安全标签映射为平面坐标系中的点，如（$i_1$，

$c_1$)；而主体依据其安全标签映射为平面坐标系中的矩形区域，如由点($i_1$,$c_1$)、($i_2$,$c_1$)、($i_2$,$c_2$)和($i_1$,$c_2$)界定的区域。同时，主体安全标签将平面坐标系划分为 9 个区域，各区域的授权结果如图 3 所示，其中 WR 表示可读可写，R 表示仅可读，W 表示仅可写，D 表示访问被拒绝。

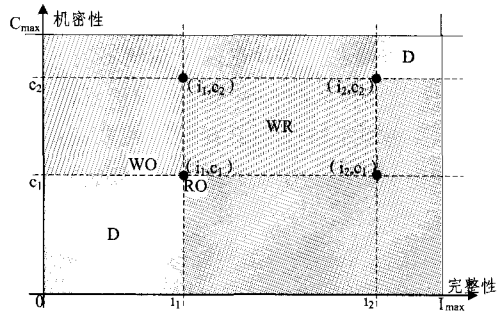


图 3　安全标签设计与授权规则

客体采用固定安全标签是为了防止信息的非法泄露和非法篡改，如以完整性属性来说明客体安全标签可变而导致的信息非法泄露问题。

主体 $A$、$B$ 与客体 $O$ 如图 4 所示，根据完整度约束关系，主体 $A$ 可以对客体 $O$ 进行写操作，信息流为 $A\rightarrow O$；主体 $B$ 可以对客体 $O$ 执行读请求，信息流为 $O\rightarrow B$。从而可能产生非法信息流：$A\rightarrow B$，导致主体 $B$ 的信息遭受非法篡改。

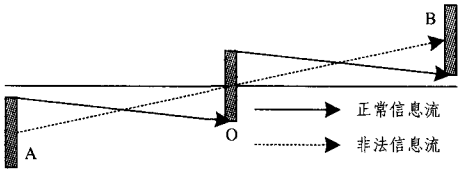


图 4　客体安全标签可变

当客体采用固定安全标签时，当且仅当主体 $A$ 和主体 $B$ 的完整度区间重叠时，才会产生从主体 $A$ 到主体 $B$（或者 $B$ 到 $A$）的正常信息流动，如图 5 所示。

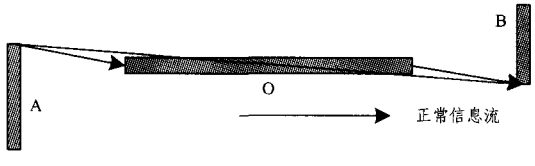


图 5　客体安全标签固定

### 3.2　安全标签的调整

安全标签体现了主体对系统资源的访问能力，以机密性属性为例，主体机密性属性由机密性上界与机密性下界界定的可变区间来体现，主体机密性属性由两要素决定：区间中点 $M$ 和区间半径 $R$，其中区间中点是区间上界与下界的数学平均值，区间半径是区间上界与下界差值的一半。因此，区间中点体现了主体平均访问能力，而区间半径则体现了主体访问范围。

在进程对文件访问控制原型系统中，进程安全标签的调整主要是依据进程可信度调整区间中点 $M$ 和区间半径 $R$，安全标签的调整包括标签更新和标签修正。

(1)标签更新

如图 2 所示，曲线中急剧下降的点称为拐点(inflexion)，也是干扰发生点。假设选取拐点前的上升阶段与拐点后的下降阶段($t_0$,$t_1$)作为研究对象，区间起点坐标为($t_0$,$k_0$)，拐点坐标为($t_i$,$k_i$)，区间的上界为 $T$(如 100)，下界为 0，则对拐点前的上升阶段与拐点后的下降阶段进行模拟的分段函数如式(1)所示。

$$f(x)=\begin{cases}1-\dfrac{1-k_0}{m_u^{(x-t_0)}}, & t_0<x<t_i\\ k_i*\dfrac{1}{m_d^{(x-t_i)}}, & t_i<x<t_1\end{cases}\tag{1}$$

式中，$m_u$、$m_d$ 分别为曲线渐近参数，通过实验来确定。进程行为状态值变化趋势如式(2)所示。

$$f'(x)=\begin{cases}(1-k_0)m_u^{(t_0-x)}*\ln m_u, & t_0<x<t_i\\ -k_i m_d^{(t_i-x)}*\ln m_d, & t_i<x<t_1\end{cases}\tag{2}$$

进程正常时，扩张安全标签区间来增加进程访问系统资源的能力；进程异常时，收缩安全标签区间来限制进程访问系统资源的能力。进程访问能力的变化幅度与进程行为状态值变化的剧烈程度正相关，与进程当前的访问能力负相关，通过方程求解得到主体安全标签变化幅度与进程行为状态值之间的关系，如式(3)所示。

$$g(x)=(\sqrt{\alpha*f(x)+\beta})'=\frac{\alpha*f'(x)}{2\sqrt{\alpha*f(x)+\beta}}\tag{3}$$

式中，$\alpha$、$\beta$ 通过实验来确定。分析可知，式(3)在上升阶段的最大值为 $g(t_0)$，在下降阶段的最小值为 $g(t_1)$，因此主体安全标签变化幅度如式(4)、式(5)所示。

$$\Delta M=\begin{cases}(T-M)*\dfrac{g(x)}{g(t_0)}, & t_0<x<t_i\\ M*\dfrac{g(x)}{|g(t_1)|}, & t_i<x<t_1\end{cases}\tag{4}$$

$$\Delta R=\begin{cases}(\dfrac{T}{2}-R)*\dfrac{g(x)}{g(t_0)}, & t_0<x<t_i\\ R*\dfrac{g(x)}{|g(t_1)|}, & t_i<x<t_1\end{cases}\tag{5}$$

式中，$M$、$R$ 为主体当前安全标签的中点与半径，$\Delta M$、$\Delta R$ 是变化幅度。在实际环境中，进程随机性以及异常突发性等导致进程行为曲线无法使用某个或者某几个确切的函数来描述，但其一定是由多个由拐点界定的上升阶段与下降阶段所构成，因此依据进程行为状态值能够实现主体安全标签的有效调整。以进程对文件读、写能力范围的变化来反映主体安全标签变化效果的示意图如图 6 所示。

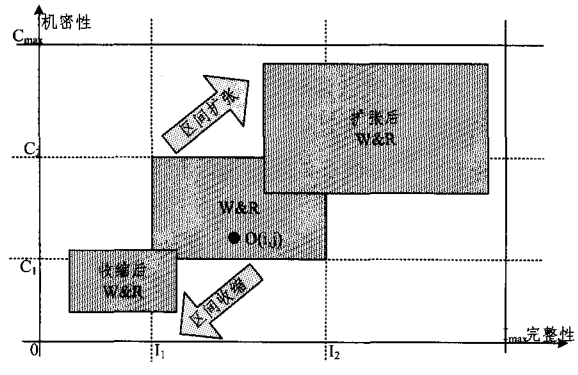


图 6　主体安全标签动态调整示意图

(2)标签修正

标签更新指在访问开始前根据进程可信度调整进程标签；标签修正指在访问结束后为防止信息的非法泄露(针对机密性)和非法篡改(针对完整性)，对进程标签进行事后调整。如图 7(a)所示，进程对文件 $a$、$b$ 具备读、写权限，假设进程从文件 $b$ 中读取信息 $m$，然后将信息 $m$ 写入文件 $a$ 中，这就导致了从机密性高向机密性低、从完整性低到完整性高的非法信息流，如图 7(b)所示。

为了避免隐藏的非法信息流，访问结束后需要根据访问对象修改进程标签。如果进程先从文件 $b$ 中读取信息 $m$，安全标签修正后，进程对文件 $a$ 的任何操作都会被拒绝，如图 7(c)所示；如果进程先访问文件 $a$，标签修正操作不会阻断进程对文件 $b$ 的访问，因为从文件 $a$ 到文件 $b$ 信息流是合法的，如图 7(d)所示。

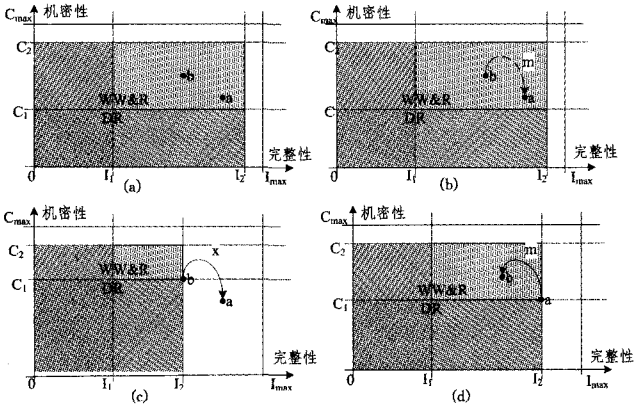


图 7　标签修正对信息流的影响

## 4　系统实现与分析

利用 Windows 文件系统过滤驱动实施可变标签的访问控制策略，建立以进程为主体、内核数据与文件为客体的简单原型系统。

### 4.1　结构设计与实现

实施可变标签访问控制策略的原型系统结构如图 8 所示，主要包括进程管理、标签管理和访问决策模块。

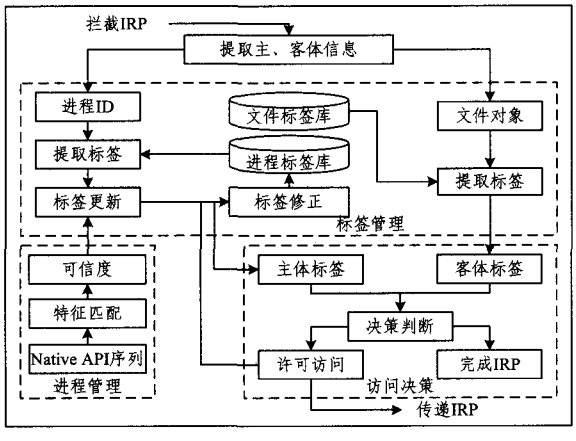


图 8　访问控制框架图

(1)进程管理

进程可信度与行为状态值的波动情况直接相关。以图 2 所示的曲线为例，选取特定阈值(如 0.8)，对高于阈值的点选用方程(1)中上升阶段函数，低于阈值的点使用式(1)中下降阶段函数进行函数变换，或者称其为一次迭代过程。

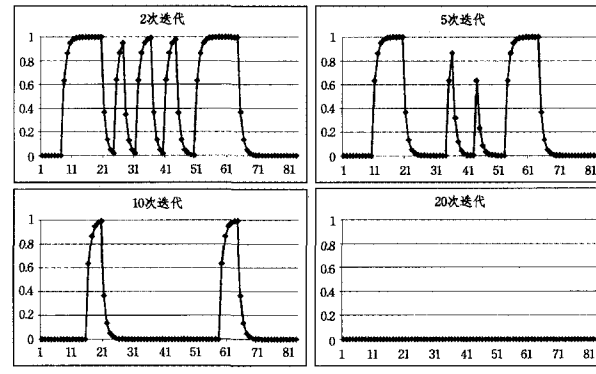


图 9　阈值为 0.8 时的多次迭代结果

多次迭代后的结果如图 9 所示，迭代次数少导致进程安全标签更新频繁；多次迭代可以降低进程行为状态值曲线的波动频率，增加曲线稳定性，但会恶化进程异常状态。综合考虑后，选择 5 次迭代的结果作为进程可信度曲线。

(2)访问决策实施

进程对文件访问的决策与实施是通过 Windows 文件系统过滤驱动来实现的，其工作方式与设备栈中的其它驱动程序的工作方式类似：接收 IPR，执行自身功能逻辑，根据需要取消、完成或传递给低层的驱动程序。其中 IRP 是 Windows 系统中用于表达 I/O 请求的核心数据结构，当内核代码要发起一个 I/O 请求时，代表该请求的 IRP 会被构造并被正确地传递到恰当的驱动程序由特定的例程来处理。

### 4.2　实验结果分析

图 10 显示了混合访问控制策略在不同安全标签下对系统可用性的影响。以完整性属性为横轴，以机密性属性为纵轴，平面直角坐标系中的阴影部分表明主体对客体的访问在 BLP 模型和 Biba 模型下能够获得一致的授权结果，其中 WR 表示可读写，WO 表示只可写，RO 表示只可读。

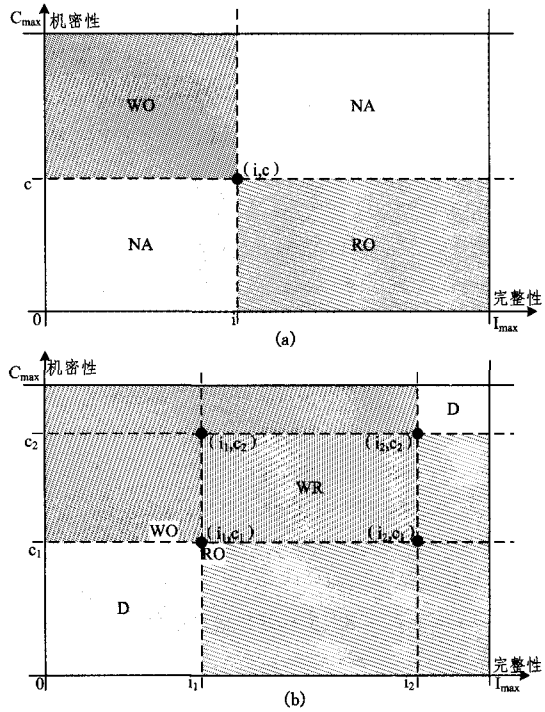


图 10　不同安全标签对系统可用性影响

图 10(a)反映了传统安全标签下主体访问资源的能力，图 10(b)反映了使用可变安全标签后主体访问资源的能力。相较于使用传统安全标签，可变安全标签的引入保证了主体对客体的访问能够得到一致、确定的访问授权，显著地提高了访问控制策略的适用范围：扩展了主体只读、只写能力范围，增添了主体可读写能力范围。

可变安全标签访问控制策略不仅显著减少了对系统可用性的影响，还能有效控制进程对系统资源的访问，实现操作系统安全加固。以机密性属性为例，进程安全标签随可信度的变化过程如图 11 所示。

原始数据子图即通过特征匹配得到的进程行为状态值曲线，其波动的剧烈程度反映了进程运行状态；进程行为状态值曲线经过 5 次迭代处理过程后得到较稳定的进程可信度曲线，如 5 次迭代子图所示；依据进程可信度曲线调整安全标签区间中点与区间半径，如安全标签半径子图所示；安全标签子图反映了不同时刻主体机密性属性上界与机密性属性下界。以机密性等级为 60 的文件为例，只有进程运行正常时才能执行对该文件的读、写操作，一旦程序异常，就失去对文件的访问操作，如安全标签子图中 API 数为 21 时所示。

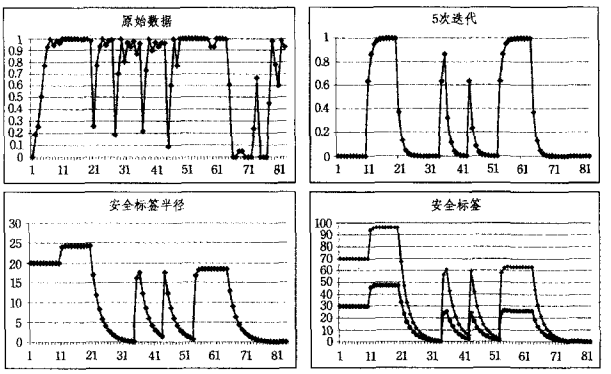


图 11　进程安全标签变化曲线

总之，进程安全标签随进程可信度的增加而扩张，随进程可信度的下降而收缩，有效限制了进程对系统资源的访问能力，降低了进程异常时的系统风险。

**结束语**　相对于经典的访问控制策略，可变标签的访问控制策略以机密性和完整性两个不同但同时存在的属性为基础，在不影响系统可用性的前提下结合了 BLP 模型保障信息机密性与 Biba 模型保障信息完整性的优点，依据进程可信度动态调整主体安全标签，消除了因 BLP 与 Biba 作用域重叠导致的系统可用性低的问题。实现基于 Windows 文件系统过滤驱动的进程对文件访问的简单原型系统，有效控制了进程对资源的访问能力，加强了 Windows 操作系统安全防护能力。在今后的研究中，将进一步研究进程可信度与安全标签之间的变化关系，并解决因多次迭代而导致的访问控制作用延时问题。

## 参 考 文 献


[1] Net Application. 2011 年主机操作系统市场调查报告[OL]. http://www.netmarketshare.com/

[2] 数据中心. 2011 年主机操作系统市场调查[OL]. http:/www.cnzz.com

[3] 黄强，沈昌祥，陈幼雷，等. 基于可信计算的保密和完整性统一安全策略[J]. 计算机工程与应用，2006，42(10)：15-18

[4] 马新强，黄羿，李丹宁. 基于扩充敏感标记的格理论模型研究[J]. 计算机工程，2009，35(21)：171-173

[5] 张俊，周正，李建，等. 基于 MLS 策略的机密性和完整性动态统一模型[J]. 计算机工程与应用，2008，44(12)：19-21

[6] 李益发，沈昌祥. 一种新的操作系统安全模型[J]. 中国科学(E辑：信息科学)，2006，36(4)：347-356

[7] 黄强，沈昌祥，陈幼雷，等. 基于可信计算的保密和完整性统一安全策略[J]. 计算机工程与应用，2006，42(10)：15-18

[8] 石文昌，孙玉芳. 多级安全性政策的历史敏感性[J]. 软件学报，2003，14(1)：91-96

[9] 郝东白，郭林，黄皓. 基于 Hook 的程序异常行为监测系统的设计与实现[J]. 计算机工程与设计，2007，28(18)：4373-4376

[10] 潘爱明. Windows 内核原理与实现[M]. 北京：电子工业出版社，2010：35-38

[11] 冯力. 主机内核级入侵检测系统的建模与分析[D]. 西安：西安交通大学，2005


(上接第 256 页)


[4] 江伟，梁家荣. Vague 集相似度量的比较研究[J]. 计算机工程与应用，2011，47(25)：30-33，64

[5] 范平，梁家荣，李天志. Vague 集之间相似度量的新方法[J]. 计算机工程与应用，2006，42(34)：70-72

[6] 叶军. 基于 Vague 集相似度量的汽轮机故障诊断的研究[J]. 中国电机工程学报，2006，26(1)：16-20

[7] 赵忠伟. 基于 Vague 集相似度量的柴油机磨损类故障诊断的研究[J]. 绍兴文理学院学报，2006，26(9)：68-72

[8] 王鸿绪，张福金. Vague 故障诊断方法在振动故障诊断中的应用[J]. 计算机工程与应用，2011，47(26)：225-227

[9] 彭安华. Vague 集的相似度量分析在材料选择中的应用[J]. 煤矿机械，2006，27(5)：891-893

[10] 叶军，徐永灿. 一种 Vague 相似度量的方案决策方法[J]. 计算机仿真，2006，23(4)：90-93

[11] 娄建国. Vague 集之间的相似度量及其在方案决策中的应用[J]. 工程设计学报，2005，12(6)：325-328，333

[12] 叶军，娄建国，李伟波. Vague 集间的相似度量分析在机构方案决策中的应用[J]. 机械设计，2005，22(6)：10-12

[13] 王鸿绪. 应用 Vague 优化决策方法对小麦新品种综合评估[J]. 计算机工程与应用，2011，47(12)：210-212

[14] 扬洁，王鸿绪. 基于完整的 Vague 模式识别方法的战场目标识别[J]. 计算机工程与应用，2011，47(4)：168-170

[15] 江军，张慧坚，王鸿绪，等. 基于 Vague 相似度量分析的椰子品种优选应用研究[J]. 江西农业学报，2011，23(2)：55-57

[16] 江军，张慧坚，王鸿绪，等. 基于 Vague 集的天然橡胶品种优化评估研究[J]. 广东农业科学，2011(6)：200-201，206