

面向测量应用的软件保护模型

徐钦桂^{1,2}, 刘桂雄², 高富荣³

(1. 东莞理工学院 计算机学院, 广东 东莞 523808; 2. 华南理工大学 机械与汽车工程学院, 广州 510640;

3. 广东省计量科学研究院, 广州 510405)

(xuqg@dgt.edu.cn)

摘要:贸易结算等测量应用要求计量软件及运行环境能有效防范包括管理员在内的各类用户的非授权篡改,但难以得到现有安全模型的有效支持。为此提出面向测量应用的软件保护模型 MBSPM, 基于角色—域—型访问控制策略分配数据访问权限, 利用强制访问控制实施数据分级保护和法制相关软件隔离, 依靠防篡改存储防止计量参数的非授权修改, 基于可信平台模块 (TPM) 保护运行环境的完整性。基于虚拟称重系统的应用实例表明, MBSPM 可支持计量应用所要求的软件保护特性, 与不实施 MBSPM 的情况相比较, 除系统启动时间增加大约 50% 之外, 文件打开和应用启动等操作的速度下降均不超过 20%。

关键词:软件保护; 安全模型; 可信计算; 计量测控; 越权操作

中图分类号: TP309.2; TP274.2 **文献标志码:** A

Software protection model for measurement applications

XU Qin-gui^{1,2}, LIU Gui-xiong², GAO Fu-rong³

(1. College of Computer, Dongguan University of Technology, Dongguan Guangdong 523808, China;

2. School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou Guangdong 510640, China;

3. Guangdong Institute of Metrology, Guangzhou Guangdong 510405, China)

Abstract: Measurement applications such as trade settlement require their metrological software and running environment protected against unauthorized modifications from attackers including management user, which is nevertheless not fully supported by the existing secure models. A measurement-oriented software protection model named MBSPM was proposed. Role-domain-type access control strategy was adopted to support authorization of data access permissions to software modules. Mandatory access control was employed to enforce multi-level data protection and separation of legal relevant software. Integrity of system software was validated by use of Trusted Platform Module (TPM). And unauthorized modification on metrology parameters was prevented with tamper-proof storage. The experimental results with a virtual weighing system show that MBSPM supports software protection features required by metrological applications. Compared with the situation without enforcing MBSPM, except for that the startup time increases by about 50%, execution speed of opening files and starting application drops by no more than 20%.

Key words: software protection; security model; trusted computing; metrology and measurement control; operation beyond authority

0 引言

贸易结算等测量应用要求计量软件及运行环境能有效防范包括管理员在内的各类用户的非授权篡改^[1]。尽管通过规范的软件过程和严格的软件测试可使计量软件获得很高的可靠性^[2], 但通用计算平台的开放结构却使计量软件面临恶意代码和越权操作的篡改威胁, 导致计量性能的可信度受到损害。针对此问题, 自 2004 年以来, 国内外计量机构和组织发布了多种计量器具软件保护规范^[3-4], 指导软件开发和验证, 提出采用法制计量手段实施计量软件保护, 建议采用封缄和动态链接库封装等方法保护计量软件和关键参数, 这些手段虽能有效防范对硬件化测量仪器的非法改动, 但难以实现基于计算机等开放平台计量器具软件系统的完整性保护。信息安全领域学者对软件保护进行了广泛的研究, 提出

Biba^[5]、DTE^[6]、Clark-Wilson^[7] 和 non-interference^[8] 等一系列安全模型, 通过实体间数据流安全检查、良构事务^[7] 和操作序列对保护域的无干扰检测等多种方法保护敏感数据免受非授权修改, 并可防范病毒和木马等恶意代码的攻击, 使大量军事和商业应用的敏感数据得到有效保护。但学术界对测量领域的软件保护研究尚不多见, 现有安全模型和保护机制对测量控制等应用中合法用户越权操作的防范问题考虑不够, 难以支持法制计量所要求的软件分离、基于模块的访问授权和软件升级保护等功能^[3-4]。以包括启动代码和操作系统在内的计算机系统平台完整性为保护目标的可信计算技术^[9] 成为近年来研究热点, 它以防篡改的独立硬件可信平台模块 (Trusted Platform Module, TPM) 和 Boot BIOS 为信任根, 结合完整性度量 and 验证进行信任链传递, 可检测系统软件的完整性状态, 但如何将可信计算和具体应用结合还有待于进一步

收稿日期: 2010-08-06; 修回日期: 2010-12-03。

基金项目: 广东省科技攻关重点项目 (2007A060304003); 广东省科技计划项目 (2007B010400046)。

作者简介: 徐钦桂 (1967-), 男, 湖南长沙人, 副教授, 博士研究生, CCF 会员, 主要研究方向: 计算机系统结构、信息安全、测量控制; 刘桂雄 (1968-), 男, 广东揭阳人, 教授, 博士生导师, 主要研究方向: 智能传感器、智能化检测; 高富荣 (1961-), 男, 广东广州人, 高级工程师, 主要研究方向: 计量检测。

研究^[10]。

为满足法制计量等测量应用所要求的软件完整性保护要求,提出一个面向计量应用的安全模型(Measurement Based Software Protection Model, MBSPM),基于计量器具软件保护规范,用形式化方法描述了访问控制、多级安全保护和软件模块自身保护的完整性保护策略。按照计量应用实例的软件结构配置模型参数,对模型的保护功能进行测试,实验结果表明MBSPM能支持计量应用所需要的软件化测量仪器完整性保护特性。

1 测量应用的软件完整性需求

计量器具软件保护规范^[3-4]将计量软件中定义或执行测量功能、表述测量特性的部分称为受法规控制的法制相关软件(legally relevant software),要求具备对非授权更改的可验证防范能力,其中用于控制和跟踪计量软件升级过程的不可升级部分称为固定法制相关软件(fix legally relevant software),其他软件部分为非法制相关软件(legally non-relevant software)。

同样,也将受法规控制的计量器具或其组件的参数定义成法制相关参数(legally relevant parameters),其中,与型式审批及检定有关的配置参数称为类型专有参数(type-specific parameters),具体设备中应受保护的可调参数和配置参数则称为设备专有参数(device-specific parameters)。法制相关软件和法制相关参数共同构成计量器具的法制相关部分,其防非授权篡改能力是计量器具稳定可靠工作的基础。法制相关数据只能通过法制相关软件进行访问,非法制相关软件如果需要访问法制相关数据,必须通过唯一软件接口调用法制相关软件的相关模块来执行,各软件模块及数据模块间的访问关系如图1所示。

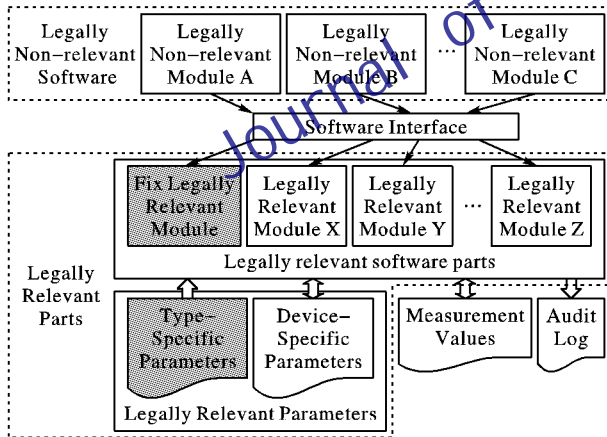


图1 计量器具软件保护结构

2 MBSPM 保护模型

先定义三种实体元素:用户(Users)是测量应用的使用、操作和管理人员;主体(Subjects)指对数据执行访问操作的进程、程序和软件模块等;客体(Objects)为可通过主体访问的对象,包括测量数据、配置参数、操作日志等数据和软件模块等,其中主体对软件模块的操作指安装、升级和删除等。

模型将基于角色—域—类型的访问控制机制与多级安全保护相结合,实施强制访问控制,通过基于公钥基础设施(Public Key Infrastructure, PKI)的身份认证和基于可信计算的信任链传递保护和验证安全模块本身的完整性,采用防篡改存储保护关键数据,使计量器具软件系统支持前述保护特性。

2.1 访问控制模型

由图1,法制相关数据只能由法制相关软件模块直接访问,即其访问权限应分配给软件模块,而软件模块的执行权限被授与经过认证的合法用户。为满足计量器具软件保护规范的要求,MBSPM采用了图2中所示的权限管理机制:1)对主体和客体分别赋予域(Domain)属性和型(Type)属性,将具有相同权能的主体置于同一保护域,而对具有相同〈主体,权限〉对的客体设置成同一类型,建立域对型的访问控制表(Domain Type Table, DTT)将对型的访问权限分配给域,将域对型的访问权限作为域中主体对该种类型客体的访问权限,从而实施面向软件模块的访问授权;2)给用户赋予角色(Roles)属性,并根据角色职能设置角色所在的保护域,由域对型的访问权限导出用户对客体的访问权限;3)位于不同域的主体间相互隔离,仅能按照域域关联表(Domain Domain Table, DDT)中指定的方式通信,使软件模块间相互隔离。

基于上述模式,可以推导各实体间的访问控制关系。推导过程中使用的表示模型中实体集和映射关系的变量有:

U 表示用户集; S 表示主体集; O 表示客体集; R 表示角色集; D 表示域集; T 表示客体类型集; $DTAM$ 表示客体访问方式集(Domain Type Access Mode set); DCM 表示域管理关联模式集(Domain Connection Mode set); $user_roles: U \rightarrow 2^R$ 表示赋予用户的角色集; $role_domains: R \rightarrow 2^D$ 表示角色所在的域集; $subject_domain: S \rightarrow D$ 表示主体所在域; $object_type: O \rightarrow T$ 表示赋予客体的类型; $DDT: D \times D \rightarrow 2^{DCM}$ 表示域域关联表; $DTT: D \times T \rightarrow 2^{DTAM}$ 表示域型访问控制表。

基于上述符号,可推导各类实体对客体的访问权限数学公式,其计算结果可作为访问控制授权的检查条件。

1) 指定主体可以指定方式访问的客体集。

$$subject_dtam_objects: S \times DTAM \rightarrow 2^O,$$

$$subject_dtam_objects(s, x) = \{o \mid o \in O \wedge$$

$$x \in DTT(subject_domain(s), object_type(o))\} \quad (1)$$

2) 可以指定方式访问指定客体的主体集。

$$object_dtam_objects: O \times DTAM \rightarrow 2^S,$$

$$object_dtam_objects(o, x) = \{s \mid s \in S \wedge$$

$$x \in DTT(subject_domain(s), object_type(o))\} \quad (2)$$

3) 指定用户可以指定方式访问的客体集。

$$user_dtam_objects: U \times DTAM \rightarrow 2^O,$$

$$user_dtam_objects(u, x) = \{o \mid o \in O \wedge \exists d \in D(d \in user_domains(u) \wedge x \in DTT(d, object_type(o)))\} \quad (3)$$

4) 可以指定方式访问指定客体的用户集。

$$object_dtam_users: O \times DTAM \rightarrow 2^U,$$

$$object_dtam_users(o, x) = \{u \mid u \in U \wedge \exists d \in D(d \in user_domains(u) \wedge x \in DTT(d, object_type(o)))\} \quad (4)$$

式(3)、(4)中的 $subject_domains: U \rightarrow D$ 定义如下:

$$user_domains(u) = \bigcup_{r \in user_roles(u)} role_domains(r)$$

5) 用户允许执行软件模块集。

$$user_modules: U \rightarrow 2^S,$$

$$user_subjects(u) = \bigcup_{r \in user_role(u)} \{s \mid subject_domain(s) \in role_domains(r)\} \quad (5)$$

2.2 多级安全保护

前述访问控制模型没有考虑客体重要性差异,并存在设置复杂和容易出错的问题,而设置不当容易导致敏感信息

的泄漏和关键参数的非授权篡改。为对不同实体实施分级保护,提出给每个主体和客体绑定一个安全级,要求主体和客体的安全级必须满足某种关系才允许访问授权,从而支持强制访问控制,其工作原理如图2的多级保护机制所示。

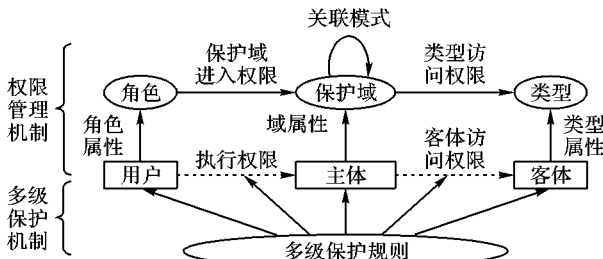


图2 MISPM 框架

实体安全级由保密级 (Security Level, SL) 和完整级 (Integrity Level, IL) 构成,并定义从主体客体集到安全级的两个映射:

$sl: S \cup O \rightarrow SL$, 实体保密级

$il: S \cup O \rightarrow IL$, 实体完整级

规定客体只能被不低于自身保密级的主体读取,仅能被不低于自身完整级的主体写入,因此客体访问需要增加两个检查条件:

$$(s, x, o) \wedge x \in \{w, r\} \Rightarrow sl(s) \geqslant sl(o) \quad (6)$$

$$(s, x, o) \wedge x \in \{a, w, c, d, u\} \Rightarrow il(s) \geqslant il(o) \quad (7)$$

其中 w, r, a, c, d, u 分别表示写入、读取、添加、创建、删除和更新操作。

将访问控制模型和多级安全机制相结合构造 MBSPM 的访问授权规则。

规则1 设 $B \subseteq S \times O \times DTAM$ 表示当前获得授权的主体对客体的访问控制权限,则每当收到访问请求 $rq(s, o, x)$ 时,系统按照以下过程进行处理:

步骤1 检查 DTT, 如果 $x \in DTT(subject_domain(s), object_type(o))$, 则转下一步, 否则拒绝访问请求;

步骤2 如果 $x \in \{w, r\}$, 则检查条件 $sl(s) \geqslant sl(o)$, 若成立, 则转入下一步, 否则拒绝访问请求;

步骤3 如果 $x \in \{a, w, c, d, u\}$, 则检查条件 $il(s) \geqslant il(o)$, 若成立, 则转入最后一步, 否则拒绝访问请求;

步骤4 授权主体 s 以方式 x 访问客体 o , 计算 $B^* = B \cup (s, o, x)$, 并用 B^* 替换 B 。

2.3 安全模块的保护

安全模块是安全模型的软硬件实现,是非授权行为的攻击焦点,面临的威胁包括利用软件漏洞旁路安全机制、利用假冒身份执行非授权操作和越权篡改关键数据等。为此,提出利用可信计算、防篡改存储和基于 PKI 身份认证实施安全模块本身的保护。

1) 基于信任链传递的软件完整性保护。利用可信计算进行计算平台完整性保护和验证的过程如图3所示。以防篡改的 BIOS Boot Block 和 TPM 作为核心可信度量根 (Core Root of Trust for Measurement, CRTM)。系统上电时, BIOS Boot Block 获得 CPU 控制权,对 BIOS 的完整性进行度量 and 验证,通过验证后将信任边界扩展到 BIOS,并将 CPU 控制传递给它;BIOS 对硬件、ROM 和 BootLoader 执行完整性度量和验证,并进行信任链传递和 CPU 控制的转移;此后,Bootloader 对 OS、OS 对其组件和应用程序执行同样的完整性度量和验证操作,最终将信任边界扩展到整个软件系统^[11],从而实现软件系统完整性保护。

件系统完整性保护。

2) 关键数据的防篡改存储。为防止利用操作系统漏洞旁路安全机制进行关键数据的非授权修改,将计量器具的关键数据保存于独立于计算机平台的防篡改安全存储设备中。关键数据包括软件完整性度量值、配置参数、定标数据和检定历史数据等。防篡改安全存储设备以 TPM 存储器扩展和独立存储硬件的形式存在,内置独立的身份认证和访问授权机制。

3) 基于 PKI 的身份认证。将计量器具的私钥、数字证书和身份认证模块存储于安全存储设备,用户私钥和数字证书存储于 USBkey。由安全存储设备采用 PKI 机制对 USBkey 进行身份认证,根据用户角色类型将对数据的访问权限授予用户,允许用户执行正常的计量操作。若认证失败,则拒绝传递计量参数,可终止应用程序的执行。

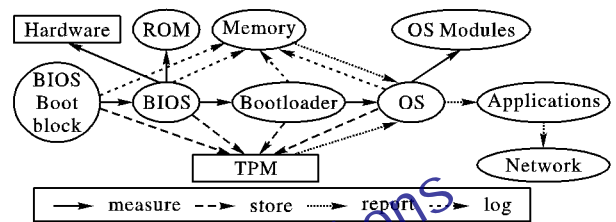


图3 信任链建立过程

3 应用实例和实验结果

为验证 MBSPM 保护功能的有效性,将其用于虚拟称重系统的软件保护。应用过程包括模型变量初始化、客体访问权限分配、安全级计算和实验验证四个步骤。

3.1 模型变量初始化

用户角色集、主体域集和客体类型集等三个模型变量需要根据虚拟称重系统工作模式和计量应用的软件保护要求进行设置。首先根据操作模式,可将用户角色集可设置为:

$$R = \{r_MetroAdmin, r_Test, r_Maint\}$$

集合中的三个元素分别表示计量管理、测量测试和系统维护角色。根据图1中的模块类别划分,将主体域集设置为:

$$D = \{d_FixLeg, d_MetroAdm, d_Test, d_Log, d_SoftInt, d_Unleg\}$$

其中各主体域分别指固定法制相关模块、计量管理模块、测量测试模块、日志管理模块、软件接口模块和非法制相关模块。客体类型集也根据图1中客体种类进行设置:

$$T = \{t_TypePara, t_DevPara, t_Data, t_Log, t_Soft\}$$

其中各元素分别代表类型专有参数、设备专有参数、测量数据、操作日志和软件模块。

3.2 客体访问权限分配

关系 $role_domains$ 、DDT 和 DTT 构成客体访问权限的分配方案,应该依据最小用户特权原则设置,并满足前述约束条件。

1) $role_domains$ 的设置条件。按照测控仪器的操作模式,具有计量管理角色的用户执行检定校准功能,而具有测量测试角色的用户执行测量测试功能,两种角色的职能不允许交叉,因此有以下约束条件:

$$\begin{aligned} d_MetroAdm &\in role_domains(r_MetroAdm) \wedge \\ \forall r \in R (r \neq r_MetroAdm \Rightarrow \\ d_MetroAdm &\notin role_domains(r)) \end{aligned} \quad (8)$$

$$\begin{aligned} d_Test &\in role_domains(r_Test) \wedge \\ \forall r \in R (r \neq r_Test \Rightarrow d_Test &\notin role_domains(r)) \end{aligned} \quad (9)$$

2) 构造 DTT 。 DTT 列出各主体域对客体类型的访问模式,由于模型按照模块和数据功能设置域和类型集合, DTT 的一种设置方式如表 1 所示,表格单元列出了主体域对客体类型的访问权限。其中,第 1 行固定法制相关模块对测量软件的读写权限表示该域中软件模块具有升级监控职能;第 2 行计量管理模块对类型专有参数的读写权限表示其具有检定职能,能修改虚拟称重系统的型式参数和定标参数,而对日志的读权限指有权查看日志、审计非法和越权操作行为;第 3 行的设置表示测量测试模块具有读取类型专有参数、修改设备专有参数和读写测量数据的权限;而第 4 行表示仅日志管理模块有权将数据写入系统日志。

表 1 域对型访问控制权限设置

主体域名	客体类型				
	$t_TypePara$	$t_DevPara$	t_Data	t_Log	t_Soft
d_FixLeg					rw
$d_MetroAdm$	rw				r
d_Test	r	rw	rw		
d_Log				a	

3) DDT 构造条件。 DDT 定义域间关联关系,允许对客体没有直接访问权限的主体通过其他主体进行间接访问。 DDT 的设置应能限制非法制相关软件仅能通过软件接口模块调用法制相关模块提供的功能访问法制相关数据,故有约束条件 (10):

$$DDT(d_Unleg, d_SoftInt) \neq \emptyset \wedge$$

$$\forall d \in D(d \neq d_SoftInt \Rightarrow DDT(d_Unleg, d) = \emptyset) \quad (10)$$

3.3 实体安全级的计算

规定实体安全级的类型为整数,安全级为 $(0,0)$ 的实体为无须保护的程序和数据,受保护软件和数据的最低安全级应为 $(1,1)$,其他模块和数据的安全级按照图 4 所示的访问关系进行计算。

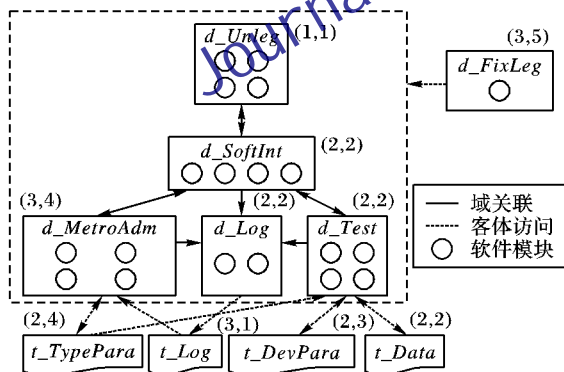


图 4 MISPM 应用实例

用 X_{dk} 和 Y_{dk} 分别表示下标 k 所指定域中主体的保密级和完整级, $k \in \{f, m, t, l, s, u\}$, 集合中各字母分别代表域 d_FixLeg 、 $d_MetroAdm$ 、 d_Test 、 d_Log 、 $d_SoftInt$ 和 d_Unleg 。同样,用 X_{di} 和 Y_{di} 分别表示为下标 i 所指定类型客体的保密级和完整级, $i \in \{t, p, d, l, s\}$ 集合中字母分别代表型 $t_TypePara$ 、 $t_DevPara$ 、 t_Data 、 t_Log 和 t_Soft 。由图 1 所示的软件完整性需求可以导出各实体安全级之间的约束方程。

1) 客体安全级约束方程。操作日志应允许任意域中主体向其添加操作日志,因而具有最低完整级,为禁止测量用户读取其内容,应拥有最高保密级。按照敏感程度,测量数据、设备专有参数和类型专有参数的完整级应依次递增。

$$IC1: Y_u > Y_{tp} > Y_{td} > Y_{tl} = 1$$

$$SC1: X_{tl} > \max(X_{td}, X_{tp}, X_u)$$

2) 主体安全级约束方程。虚拟称重系统的整个软件系统都应受到保护,其中的非法制相关模块具有最低保护需求,因而其安全级应为 $(1,1)$ 。固定法制相关模块不可升级,任何其他实体不能更改其内容,故具有最高安全级。其他模块安全级介于二者之间。因而:

$$IC2: Y_{df} > \max(Y_{ds}, Y_{dm}, Y_{dl}, Y_{dd}) \geq \min(Y_{ds}, Y_{dm}, Y_{dl}, Y_{dd}) > Y_{du} = 1$$

$$SC2: X_{df} \geq \max(X_{ds}, X_{dm}, X_{dl}, X_{dd}) \geq \min(X_{ds}, X_{dm}, X_{dl}, X_{dd}) \geq X_{du} = 1$$

3) 客体访问安全级约束方程。根据式 (6) 和式 (7),读、写操作中的主体的保密性级别 (完整性级别) 应不小于相应客体的保密性级别 (完整性级别)。分析表 1 中域对型的访问权限,可得以下不等式方程:

$$IC3: \begin{cases} Y_{dm} \geq Y_u \\ Y_{dl} \geq Y_u \\ Y_{dt} \geq \max(Y_{tp}, Y_{td}) \\ X_{dm} \geq \max(X_u, X_{tl}) \\ X_{dl} < X_{tl} \\ X_{dt} \geq \max(X_{tp}, X_{td}, X_{tm}) \\ X_{du} < \min(X_{tp}, X_{td}, X_{tm}, X_u) \end{cases}$$

解 $IC1 \sim IC3$ 和 $SC1 \sim SC3$ 组成的不等式方程组获得各主体的安全级解集,可满足图 1 的软件保护要求。从数据访问灵活性角度取其中最小数值解作为各主体和客体的保密级和完整级,并附在图 4 各域和型图标旁边。

3.4 实验环境与实验结果

假定实验用虚拟称重系统软件保护有关硬件由四部分构成:计算机、TPM、防篡改存储模块和 USB key,其结构如图 5 所示。

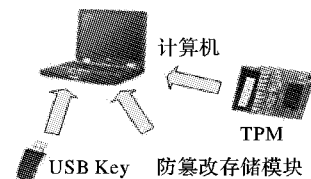


图 5 虚拟称重系统实例硬件结构

因 MBSPM 的实施涉及操作系统内核安全模块的修改,要求系统内核开源,故操作系统选用 SELinux (Security-Enhanced Linux),其内核内置了域—类型增强 (Domain and Type Enforcement, DTE)、基于角色访问控制 (Role Based Access Control, RBAC) 和 Biba 等模型的安全机制,并易于集成 MBSPM 的保护功能。

虚拟称重系统的重量单位、秤容量、传感器容量及其灵敏度等可划分为类型专有参数,而误差修正参数、误差补偿参数和量程参数等为设备专有参数。这些参数保存于防篡改存储模块以防止非法修改。

对该虚拟称重系统的软件保护功能进行测试,结果如表 2 所示。系统启动过程中从 TPM 开始测量和验证 BIOS、操作系统和固定法制相关模块的完整性,如因篡改而验证失败会终止信任链传递,停止启动系统。其他计量软件模块的完整性由固定法制相关模块进行测量和验证,如遭篡改则称重系统拒绝启动并记录日志。计量参数的非授权修改操作将导致

失败并记录日志。

实施 MBSPM 时,执行速度受影响的操作主要有系统启动、称重系统启动和文件打开等需要 TPM 或防篡改存储参与的操作,表 3 所示的测试结果表明,与不实施 MBSPM 相比,除系统启动时间增加不超过 50% 外,另外两种操作执行时间仅增加不超过 20%。

表 2 MBSPM 保护功能和性能实验结果

用户角色	操作	系统响应
r_MetrolAdm	修改秤容量	成功, 记录日志
r_Test	修改秤单位	失败, 记录日志
r_Test	修改量程参数	成功, 记录日志
无效角色	运行称重系统	失败, 记录日志
r_MetrolAdm	更改系统软件	系统不启动
r_MetrolAdm	更改固定法制相关模块	系统不启动
r_MetrolAdm	更改其他计量软件模块	称重启动失败, 记录日志

表 3 实施 MBSPM 对系统操作的影响

是否实施 MBSPM	消耗时间/s		
	称重应用启动	打开 1 MB 文件	系统启动
不实施	2.00	1.05	28
实施	2.50	1.20	40

4 结语

基于开放计算平台的测量仪器软件保护是其推广应用有待解决的关键问题。MBSPM 基于角色-域-型访问控制实现灵活高效的权限分配,可将软件模块作为数据访问权限基本分配单位,采用强制访问控制实现软件和数据的分级保护,将法制相关软件分离、法制相关数据的访问保护和软件升级的保护管理转换成常规的数据访问授权,增强了模型的适应性。利用可信计算和防篡改安全存储保护计算机平台本身的

安全性,使基于计算机的测量仪器可满足软件完整性保护要求,其保护功能和运行效率表明所提出的模型为测量应用的软件保护和验证提供一条可行的途径。然而模型要求将保护机制加入操作系统内核,其计算平台目前仅限制为开源系统。未来将研究广泛使用的非开源 Windows 环境下测量应用的软件保护问题。

参考文献:

- [1] 原和平,赵凯,赵燕.电子衡防作弊系统的研究与应用[J].中国有色金属,2008(4):54-56.
- [2] 单锦辉,姜瑛,孙萍.软件测试研究进展[J].北京大学学报:自然科学版,2005,41(1):134-145.
- [3] OIML. OIML D 31: General requirements for software controlled measuring instruments [S], 2008.
- [4] WELMEC 7.2 Issue 3, 2008, Software Guide (Measuring Instruments Directive 2004/22/EC) [S], 2008.
- [5] 张相铎,孙玉. Biba 模型中严格完整性政策的动态实施[J].计算机研究与发展,2005,42(5):746-754.
- [6] JI QINGGUANG, QING SIHAN, HE YEPING. A formal model for integrity protection based on DTE technique [J]. Science in China Series F: Information Sciences, 2006, 49(5):545-565.
- [7] 何建波,郭新,卿斯汉.一种基于 TE 技术实现 Clark-Wilson 模型的方法[J].电子学报,2008,36(2):216-223.
- [8] 司天歌,谭智勇,戴一青.一种对多级安全模型安全性的分析方法[J].计算机研究与发展,2008,45(10):1711-1717.
- [9] Trusted Computing Group [EB/OL]. [2010-09-22]. <http://www.trustedcomputinggroup.org/>.
- [10] REN JIANGCHUN, DAI KUI, WANG ZHIYING. Analysis and suggestion on TCG specifications [J]. Journal of Communication and Computer, 2006, 3(7):1-6.
- [11] 谭良,徐志伟.基于可信计算平台的信任链传递研究进展[J].计算机科学,2008,35(10):15-18.

(上接第 965 页)

3 结语

隐藏容量、不可感知性和鲁棒性是信息隐藏系统的关键性指标之一,选择不同的 DCT 系数对 DCT 域隐藏算法的这些指标影响很大。如何选择系数才能使得 DCT 域信息隐藏算法有较好的性能,学者们有不同的看法,不过目前学者们主要考虑的是 DCT 系数对隐藏信息的鲁棒性的影响,而很少考虑对嵌入容量的影响。本文分析了不同 DCT 系数的视觉感知特性和 DCT 逆变换的相互干扰性对嵌入容量的影响,理论分析和仿真实验结果均表明嵌入容量随着 DCT 系数从高频至低频依次减少。进一步通过分析 JPEG 压缩不变性,得出了嵌入信息抗压缩的鲁棒性与嵌入位置无关的结论,利用这一结论还可将信息嵌入到随机选择(如利用混沌映射)的 DCT 系数上,在保持鲁棒性的前提下提高安全性。综合嵌入容量和鲁棒性两项指标,得出了在相同的抗压缩的鲁棒性和不可感知性约束条件下,要有较高的嵌入容量,就应选择高频 DCT 系数作为嵌入载体这一结论,可为研究有高嵌入容量要求的隐藏算法提供参考。

参考文献:

- [1] 张秋余,刘洪国,袁占亭.基于图像局部稳定性的 LSB 隐藏信息检测算法[J].通信学报,2009,30(11):37-43.

- [2] ASLANTAS V. An optimal robust digital image watermarking based on SVD using differential evolution algorithm [J]. Optics Communications, 2009, 282(5):769-777.
- [3] 楼偶俊,钮旋.基于特征点模板的 Contourlet 域抗几何攻击水印算法研究[J].计算机学报,2009,32(2):308-316.
- [4] 肖亮,韦志辉.脊波域稳健性水印嵌入算法与可靠性分析[J].南京理工大学学报:自然科学版,2008,32(4):411-415.
- [5] COX I J, KILIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 1997, 6(12):1673-1687.
- [6] 黄继武,SHI Y Q,程卫东.DCT 域图像水印:嵌入对策与算法[J].电子学报,2000,28(4):57-60.
- [7] LIN C-C, SHIU P-F. DCT-based reversible data hiding scheme [J]. Journal of Software, 2010, 5(2):214-224.
- [8] 尤新刚,郭云彪,周琳娜.峰值信噪比不宜用来评价信息隐藏技术[C]//CIHW 2000/2001:全国第三届信息隐藏学术研讨会论文集.西安:西安电子科技大学出版社,2001:51-56.
- [9] 楼斌,沈海斌,赵武锋,等.基于失真模型的结构相似度图像质量评价[J].浙江大学学报:工学版,2009,43(5):864-868.
- [10] XIE JIANQUAN, XIE QING, HUANG DAZU, et al. Research on imperceptibility index of image information hiding [C]//NSWCTC: Proceedings of the 2th International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington, DC: IEEE Computer Society, 2010, 2:49-53.