第 34 卷 第 4 期 计 算 机 工 程 2008 年 2 月
Vol.34 No.4 Computer Engineering February 2008
·博士论文· 文章编号：1000—3428(2008)04—0001—03 文献标识码：A 中图分类号：TP316

基于可信计算的终端数据分类保护

王 飞[1]，吕辉军[2]，沈昌祥[3]
(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 国防科技大学计算机学院，长沙 410073；3. 海军计算技术研究所，北京 100036)

摘 要：根据当前的终端数据保护面临的问题，提出一种基于可信计算和 DBLP 模型的终端数据分类保护方案。给出在 DBLP 模型下主体对客体的读、写规则，以及迁移到移动介质上的客体保密原则，避免因无法实现进程隔离而带来的信息泄露。密文集客体的安全由 TPM 支撑的 TSS 接口实现密封存储保护。

关键词：可信计算；BLP 模型；终端；安全

Terminal Categorial Data Protection Based on Trusted Computing

WANG Fei[1], LV Hui-jun[2], SHEN Chang-xiang[3]
(1. School of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004; 2. School of Computer, National University of Defence Technology, Changsha 410073; 3. Naval Institute of Computing Technology, Beijing 100036)

【Abstract】 According to the current problems of terminal data protection, this paper puts forward a kind of terminal categorial data protection scheme based on trusted computing and DBLP. It gives some read or write rules based on DBLP, and security principles to the objects which are written in mobile mediums. It can avoid information leak by unimplemented process isolation. The security of objects in cryptograph set is provided by TSS interfaces based on TPM.

【Key words】 trusted computing; BLP model; terminal; security

1 概述

终端不仅是人们日常工作的主要平台，还是创建和存放敏感信息的源头，绝大多数的信息泄漏事件也是从终端发起的。然而目前绝大部分终端软硬件体系结构简化，硬件配置、资源很容易被篡改或误用，恶意代码很容易利用操作系统的漏洞将敏感信息泄漏出去，信息盗取者也很容易绕开操作系统的保护非法获取信息的访问权。

终端的数据保护主要集中在两个方面：一方面是数据“存储的安全可信”;另一方面则要考虑数据访问的“环境安全可信”。“存储的安全可信”是指存储在终端的重要数据都以密文形式存在，防止泄密和客体重用。“环境安全可信”是指操作系统运行环境的可信，具体访问数据的应用或服务的安全可信，以及数据访问实施的安全策略可信。这是因为操作系统是数据访问的大环境，只有首先保证操作系统的可信，才能保证运行在操作系统之上的应用可信；数据访问的主体是应用或服务，只有主体安全可信，才能保证在访问数据的同时保证数据的安全；安全策略是主体访问数据乃至数据安全存储的关键，没有安全策略则无法实施对数据存储及访问的控制。

可信计算组织TCG/TCPA[1]提供的基于硬件的数据安全存储和完整性验证解决方案已经成为目前信息安全领域研究的热点。可信计算平台指利用可信计算技术提供的机制和方法，部署了TCPA相应软硬件(包括可信平台模块TPM[2]和可信软件栈TSS)的计算平台。它的新特点为终端数据安全可靠的分类保护提供了软硬件支持。

BLP模型[3]通常是处理多级安全信息系统的设计基础。主体在处理密级数据时，要防止处理高保密级数据的程序把信息泄露给处理低保密级数据的程序。BLP模型的出发点是维护系统的保密性，有效地防止信息泄露。

目前相关的安全产品，如卫士通的“一KEY通”[4]和瑞达的“电脑守护神”[5]等，都采用“文件保密柜”、“强制访问控制”等安全策略对数据的存储通过加密进行保护。并且，在这些数据保护方案中，所有的数据(包括非保密数据和保密数据)都可以通过端口(USB口、光驱、网卡等)拷贝到平台外部，这是合理但不安全的。

文章立足于终端，从源头抓起，利用可信计算技术和DBLP 模型共同构筑全面高效的终端数据分类保护系统。

2 基于改进 BLP 模型的数据分类保护模型

基于可信计算的终端数据分类保护方案中以 TPM 与可信 BIOS 共同组成整个系统的“可信根”，由其分别对操作系统内核、应用和服务进行可信验证，完成可信链的传递，保证操作系统的环境可信。由操作系统内核对应用/服务进行代码级的静态检查和其加载动态库的检查，保证应用/服务的安全可信。同时以安全策略来保证数据访问过程的可信，以TPM 为硬件支持来保证数据存储的安全可信。因此，基于可信计算的数据分类保护模型如图 1 所示。

在文章中安全模型是基础，可信计算技术是支撑。本文不对“操作系统运行环境可信”和“应用可信”作讨论，详见另文。

基金项目：国家“863”计划基金资助项目(2002AA1Z2101)
作者简介：王 飞(1979－)，男，博士研究生，主研方向：信息安全，安全操作系统；吕辉军，博士研究生；沈昌祥，院士、博士生导师
收稿日期：2007-03-30 **E-mail：**wangfei791009@163.com

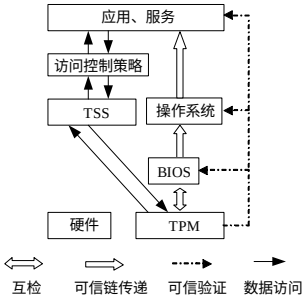

图 1　终端信息分类保护结构

2.1　BLP 模型

定义 1　S 表示主体集合；$S_T \subseteq S$ 表示可信主体集合；$S' = S - S_T$ 表示非可信主体集合；O 表示客体集合；C 表示密级集合；K 表示范畴集合；L 表示安全级集合 $L=\{(C_i,K_j)\,|\,C_i \in C \wedge K_j \in K\}$，设 $L_1=(C_1,K_1)\in L$，$L_2=(C_2,K_2)\in L$，则 $L_1 \geq L_2$ 表示 $(C_1 > C_2 \wedge K_1 \supseteq K_2)$。

定义 2　$A=\{r,w,e,a\}$ 表示访问属性；r 表示只读；w 表示读写；a 表示只写；e 表示执行；R 表示请求集合；$D=\{yes,no,error,?\}$ 表示判定结果；W 表示进行判定的规则集合。

定义 3　$V = B\times \boldsymbol{M} \times F \times H$ 表示系统状态集合，$B = 2^{(S\times O\times A)}$ 表示 $(S\times O\times A)$ 的幂集；$\boldsymbol{M}$ 为存取矩阵，由元素 $m_y \in A$ 组成，m_y 表示主体 s_i 对客体 o_j 具有的访问权；$F \subseteq L^S \times L^O \times L^S$ 表示访问类函数，$\forall f \in (f_s, f_o, f_c)$，其中，$f_s$ 表示主体的安全级函数，f_o 表示客体的安全级，f_c 表示主体的当前安全集函数；H 表示当前客体的层次关系。

系统的任一状态 $v=(b,\boldsymbol{M},f,H)\in V$，其中，$b=(s_i,o_j,x)\in B$，$x \subseteq m_y$。

特性 1　简单安全特性(ss-特性)：状态 $v=(b,\boldsymbol{M},f,H)\in V$ 满足简单安全特性 *iff* 对所有 $(s,o,x)\in b$

$x=a$ 或 $x=e$　(只写或执行)

$x=w$ 或 $x=r$，且 $f_s(s)\geq f_o(o)$ (读写或只读)

特性 2　*-特性：状态 $v=(b,\boldsymbol{M},f,H)\in V$ 满足*-特性 *iff* 对所有 $(s,o,x)\in b$ ：

(1) $x=r \Rightarrow f_s(s)\geq f_o(o)$。

(2) $x=a \Rightarrow f_o(o)\geq f_s(s)$。

(3) $x=w \Rightarrow f_s(s)\geq f_o(o)$。

特性 3　自主安全特性(ds-特性)：状态 $v=(b,\boldsymbol{M},f,H)\in V$ 满足自主安全特性 *iff* 对所有 $(s_i,o_j,x)\in b$，$x\in m_y$。

定义 4　当 v 状态同时满足 ss-特性、*-特性和 ds-特性时，称 v 为安全状态。状态序列 Z 是一个安全状态序列 *iff* $t\in T$ 对于每一个 $t\in T$，$z\in Z$，都是安全状态。

定义 5　系统是 $\sum(R,D,W,z_0)$ 一个安全系统 *iff* 系统的每一个状态 $(z_0,z_1,\cdots,z_n)$ 均为安全状态。

由于 BLP 模型过于严格，使得用户的使用受到极大的限制。在实际的工作环境中，一个用户可能在操作高保密级的数据的同时，也需要同时操作低保密级的数据。如高保密级用户需要批改下级的文件等，按照 BLP 模型，用户将无法“写”低保密级的数据。并且受目前操作系统安全的限制，进程之间无法实现隔离，有利用内存共享泄露秘密数据的可能。因此，需要相应修改 BLP 模型，调整其适用性，使之符合用户的操作。

2.2　DBLP(Developed BLP)模型

BLP 模型中可信主体可以不受*-规则限制向下写低保密级客体，但其定义不够清晰。本文给出方案中的明确定义。

定义 6　可信主体是指经过可信链建立过程经过 TPM 校验的系统内核级进程，及部分指定的经过代码静态校验和其加载动态库经过白名单检查的应用或服务进程。即可信主体是经过严格完整性检查，从而保证其行为可信；且在安全策略的控制下，可信主体不会破坏系统的保密性，并且信任可信主体可以操作某保密级以下的数据。

定义 7　保密性集合 C 分为密文集 C_1 和明文集 C_2，即 $C=C_1\cup C_2$。其中，C_1 又分为“分级密文” C_{1m} (绝密、机密和秘密，且密级：绝密>机密>秘密)和 C_{1p} (私有密文)；且所有 C_1 元素保密级别高于 C_2。

特性 4　*'-特性：状态 $v=(b,\boldsymbol{M},f,H)\in V$ 满足*-特性 *iff* 对所有 $(s,o,x)\in b$

(1) $x=r \Rightarrow f_s(s)\geq f_o(o)$。

(2) $x=a \Rightarrow f_o(o)\geq f_s(s)$。

(3) $x=w \Rightarrow (\neg\exists o'\in O, f_o(o') \leq f_o(o)\wedge((s\,r\,o')\vee(s\,w\,o'))) \wedge f_s(s)\geq f_o(o)$

或 $(\neg\exists o'\in O, s'\in S, Se(o')\leq Se(o)\wedge((s'\,r\,o')\vee(s'\,w\,o'))) \wedge f_s(s')\geq f_o(o)$。

即一个主体 s“写”客体 o，当且仅当不存在另外一个客体 o' 且 o' 保密级比 o 保密级高，s“读”或“读写” o'；或不存在一个客体 o' 和一个主体 s'，且 o' 保密级比 o 保密级高，s'“读”或“读写” o'。可信主体不受此约束。

改进后的模型可以做到主体能够“读”所有保密级低的客体；同时可以保证若当前有比该主体待“写”客体保密级高的客体被访问的情况下，不允许其“写”操作。这是因为即使满足了 BLP 模型，但由于当前操作系统环境下不能够做到进程间的完全隔离，会存在进程之间的内存泄露而导致的信息泄密情况发生。

因此，具体在操作环境下的控制规则如下：

规则 1　$\forall o\in O \wedge f_o(o)\in C_{1m}$，不允许复制 o 得到 o'，使得 $f_o(o')\leq f_o(o)$。

即不允许任何保密属性属于 C_{1m} 集合中的客体被降级。

规则 2　$\forall o\in O \wedge f_o(o)\in (C_2\cup C_{1p})$，当发送到移动介质一个副本 o'，且强制使得 $f_o(o')\in C_1$。

所有私有文件或明文文件被存储到移动介质时，必须以密文形式存在。

规则 3　$\forall o\in O \wedge f_o(o)\in C_{1p}$，可以得到 o 的一个副本 o'，且 $f_o(o')\in (C_2\cup C_{1m})$。

允许所有私有文件可以被复制为分级文件或明文文件。

规则 4　$\forall s\in S_T$，不受上述规则约束。

因为操作系统环境下系统或某些应用的日志进程实时记录当前用户的行为，所以必须使其不受影响。

2.3　DBLP 与 BLP 模型的比较

DBLP 模型与 BLP 模型相比，有以下几个方面的优点：

(1)能够在目前的硬件环境和操作系统环境下实现“保密性”规则。BLP 模型由于限制过于严格，因此无法在目前的操作环境下实施。因为在实际的工作环境中，一个用户可能在操作高保密级的数据的同时，同时也需要操作低保密级的数据。

而 DBLP 模型不仅可以在目前的操作系统环境下实现；而且能够在机密性客体被访问的情况下，可以有效防止由于

无法实现进程隔离而导致的高保密级客体信息泄露的问题。

(2)明确了“可信主体”的概念。BLP 模型虽然提出了“可信主体”的概念，但并没有明确指出哪些主体属于可信范畴。因为可信主体可以不受*-规则限制，所以在限制主体访问客体时没有指导意义。

DBLP 模型指出可信主体都是经过可信校验，并且不会产生恶意行为；同时可信主体的明确能够使得操作系统在 DBLP 模型实施的情况下正常工作。如：操作系统的日志进程 smlogsvc.exe 及其他重要应用的日志进程在经过可信校验后都属于可信主体，它们需要实时地记录日志文件，即使在有保密级客体被访问情况下也不能限制其正常的记录操作。

(3)可以解决通过移动设备的数据迁移问题。在 BLP 模型中，高保密级主体不能写低保密级客体。也即在实际工作环境中依照 BLP 模型，高保密级用户将无法通过移动设备将数据迁移到其他平台上工作，这给用户造成了极大的不便。

DBLP 模型指出，可以通过对写入到移动设备上的数据进行强制加密后迁移。而且在目的终端上对移动设备上的迁移数据解密，只有拥有相应保密级别的终端才可以对其实施 UNSEAL 操作。这不仅能够有效防止高保密数据的泄露，同时方便了用户的正常使用。

3 基于可信计算的模型实施

3.1 TPM 和 TSS

可信计算技术基于 TPM 安全模块，向操作系统提供密钥存储、密码算法，以及可信的强制访问控制调用等服务。TPM 就像一道门，提供了一级保护存储的命令(SEAL, UNSEAL 操作等)以虚拟安全存储空间的方式持久保存任意数据量的保密信息。具体在 TPM 外使用这些持久存储信息的函数如密钥生成与保存，关联用户等由操作系统和应用程序自己定义，TPM 是系统 TCB 的重要组成部分。

TSS(TCG 软件栈)是支持 TPM 的台上支撑软件，TSS 规定了 TPM 与操作系统结合的方式与接口。TSS 为应用提供敏感信息(密钥、证书、认证信息、操作日志等)密封和持久存储的功能，作为一种可信服务。密封存储实施的基本原理基于存储根密钥(SRK)，它是公钥/私钥对，私钥不离开 TPM，在需要为数据加密时用公钥加密(SEAL 操作)，用 TPM 保存的私钥解密(UNSEAL 操作)，因此，只能通过 TPM 解密。

在可信计算环境下以 TPM 为基础、TSS 为支撑，以密封存储和访问控制实现该模型下数据分类保护实施。

3.2 数据分类保护实施

“分组密文”(包括绝密、机密和秘密)的加/解密密钥由操作系统生成；私有密文的加/解密密钥由用户自己生成。对数据的存储和访问过程由按照 DBLP 模型实施。其流程如图 2 所示。

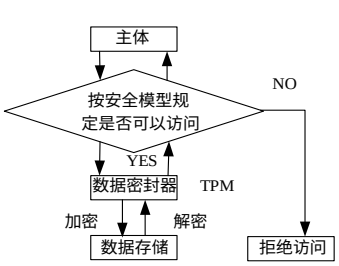

图 2 数据分类保护流程

对于密级数据保护的密钥由操作系统自动生成，公钥公开，私钥由 TPM 保存。

在实际的操作系统环境下，用户的操作可以简化为两类：读操作和写操作。下面对这两类操作的实施流程程加以说明：

(1)读操作

主体 s 在读客体 o 时：

1)根据主体 s 、客体 o 的保密级别作判断，如果主体 s 的保密级大于或等于客体 o 的保密级则允许其读执行 2)，否则拒绝读操作；

2)操作系统判断用户当前读客体的保密属性。若其属于密文集，则通过 TSS 提供的接口透明地取出 TPM 中存储的私钥，对客体进行 UNSEAL 操作并返回给主体；若其属于明文集，则直接返回给主体。

(2)写操作

主体 s 在写客体 o 时：

1)判断当前操作系统环境下是否有对客体 o' ($(f_o(o) < f_o(o')) \wedge (f_o(o') \in C_1)$)的操作；若存在，拒绝执行“写”操作；否则执行 2)；

2)若客体 o 的保密性级别 $f_o(o)$ 是当前所有被访问客体中最高，则执行“写”操作；否则拒绝“写”操作；

3)若客体 o ($f_o(o) \in C_{1p} \cup C_2$)是客体 o' ($f_o(o') \in C_{1m}$)的一个副本，则拒绝“写”操作；

4)若客体 o 写入移动介质，则强制其保密级属性 $f_0(o) \in C_1$ 。

在允许执行“写”操作时，同样操作系统首先判断用户写客体的保密属性。若其属于密文集，则通过 TSS 提供的接口透明地取出客体对象存储的公钥，对客体进行 SEAL 操作后，写入磁盘；若其属于明文集，则直接写入磁盘；若属于迁移到移动介质上的客体，则由 TSS 提供的接口透明地取出迁移密钥，对客体进行 SEAL 操作后，写入移动介质。

4 结束语

基于可信计算和 DBLP 模型的终端数据分类保护方案体现了操作系统安全的机密性特性，可以实现对终端数据的存储保护和访问安全。在下一步工作中，考虑终端数据的可信迁移问题。所有终端数据迁移到移动介质上都必须以密文形式存在；并依具“全程 BLP”思想实现迁移数据在其他平台上的 UNSEAL 操作和使用，即只有迁移目的平台拥有足够的保密性级别时，才允许其对迁移数据执行 UNSEAL 操作和使用。

参考文献

[1] TCG. Trusted Computing Group(TCG) Main Specification Version 1.1a[EB/OL]. (2001-09-10). http://www.trustedcomputinggroup.org/ downloads/tcg spec 1.1b.zip.

[2] Trusted Computing Group. TPM Main Specification: Design Principles v1.2[EB/OL]. (2003-10-20). https://www.trusted computinggroup.org.

[3] Bell D E, LaPadula L J. Secure Computer System：A Mathematical Model[R]. The MITRE Corporation, Technical Report: M74-244, 1973.

[4] 卫士通．一Key通[EB/OL]. (2006-10-20). http://www.westone.com.cn/2006-10.

[5] 瑞　达．电脑守护神[EB/OL]. (2006-10-20). http://www.jetsec.com.cn.