第 34 卷 第 15 期 计 算 机 工 程 2008 年 8 月
Vol.34 No.15 Computer Engineering August 2008
·博士论文· 文章编号：1000—3428(2008)15—0007—03 文献标识码：A 中图分类号：TP316

基于 TPM 的终端数据可信迁移研究

王 飞[1,2]，李 勇[1]，郭东文[2]
(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 装备指挥技术学院，北京 101416)

摘 要：提出一种终端数据可信迁移方案以解决数据无防护地流入/流出终端所带来的安全问题。根据“全程 BLP 规则”对待流入/流出的数据进行安全检查，只允许符合安全策略的数据迁移，由 TPM 负责将其加密/解密。介绍实现框架并分析其安全性。该方案可以保证迁移数据的机密性和可控性。

关键词：可信计算；可信平台模块；终端数据；可信迁移

Research on Trusted Transfer of Terminal Data Based on TPM

WANG Fei[1,2], LI Yong[1], GUO Dong-wen[2]
(1. Electronic Techndogy Institute, PLA Information Engineering University, Zhengzhou 450004;
2. Academy of Equipment Command & Technology, Beijing 101416)

【Abstract】This paper presents a method of terminal data trusted transfer to solve the security problems, which are caused by data flowing in or out of terminals. According to “overall BLP model”, the data to flow in or out of terminals are checked, and only those matching the security policies can be transferred, which are encrypted or decrypted by TPM at the same time. It gives an implementation framework of the method, and analyzes its security. The method can insure that transferred data is confidential and controllable.

【Key words】trusted computing; Trusted Platform Module(TPM); terminal data; trusted transfer

1 概述

使用移动存储设备带来的不安全性已经引起了科技工作者极大的关注，对其研究集中在以下 2 个方面：

(1)禁止使用网络或严禁涉密计算机上网，禁止使用可移动存储器等措施[1]。这种方式严格限制用户使用网络或移动存储设备，给用户带来使用上的不便。事实证明，通过规章制度来防止信息泄露已经不能满足要求，必须采用技术手段保证敏感数据的安全性。

(2)简单地通过加密方式进行处理。目前采用的技术手段主要是加密。通过对移动设备上的内容加密，可以使其不能被非法用户使用。但是对于数据迁移而言，迁入平台与迁出平台的密钥分发与共享还有待解决。而在目前的普通终端平台上无法解决加密密钥的产生、更换以及密钥本身的保密等密钥管理问题，使得这一措施难以实现[2]。

以上 2 种方案都没有考虑数据迁移出平台后的访问控制管理问题。如果一个数据在终端 A 是受控数据，即只有指定的合法用户可以访问，若只是简单地将其迁移出到其他平台，它将会成为一个非受控的文件，导致一定程度的信息泄露。可信计算技术及可信计算平台的提出为解决该问题提供了新的思路。本文提出可信计算平台上基于可信平台模块(Trusted Platform Module, TPM)的数据可信迁移方案。

2 TPM 及可信计算平台

2.1 可信平台模块

可信计算技术基于 TPM[3]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 提供了一级保护存储的命令(SEAL, UNSEAL 等操作)，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。

根据密钥的使用范围，TPM 管理的密钥可以分为 3 类：平台身份类密钥，平台存储类密钥和用户类密钥。而平台身份类密钥又可分为背书密钥(Endorsement Key, EK)、身份认证密钥(Attestation Identity Keys, AIK)和平台加密密钥(Platform Encryption Key, PEK)等。

应用程序在使用 TPM 的功能时并不直接与 TPM 交互，而是通过被称为 TSS(TCG Software Stack)的软件栈与 TPM 进行交互。如图 1 所示，TSS 是可信平台模块与使用 TPM 功能应用程序之间的支撑软件，提供对 TPM 的访问、安全认证、密码学服务和管理 TPM 的资源等重要功能。

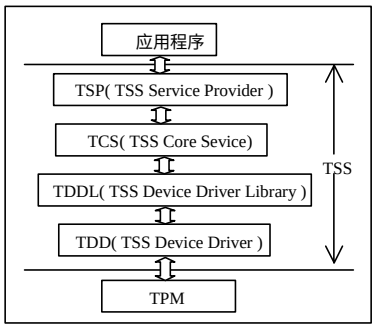


图 1 TSS 模块

2.2 可信计算平台

可信计算平台[4-5]是基于 TPM，以密码技术为支持、安全操作系统为核心的计算机硬件平台。完整的可信计算平台系统由平台管理中心(Platform Management Center, PMC)和

基金项目：国家“863”计划基金资助项目(2006AA01Z440)
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；李 勇，博士研究生；郭东文，讲师
收稿日期：2007-09-20 **E-mail：**wangfei791009@163.com

可信计算平台终端组成。

(1)平台管理中心负责安全管理和密码管理。平台管理中心根据可信计算平台终端的人员角色、信息资源、密钥需求及安全需求等各方面信息进行综合分析，生成符合终端安全的安全策略和所需的各类密钥配置。同时负责对各终端进行安全策略及密码配置的维护。

(2)可信计算平台终端负责安全策略的预处理和实施。可信计算平台终端通过人工或网络获取安全策略和密钥配置，将密钥配置到本地 TPM 并加密保存安全策略。然后安全操作系统按照安全策略对用户的操作进行控制。

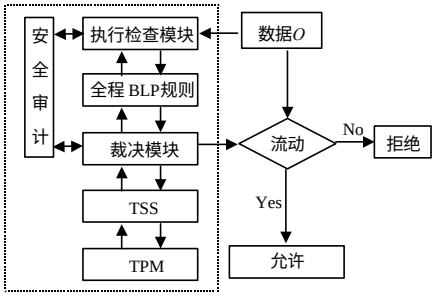
可信计算平台是本方案的硬件基础，其定义如下：

定义 1 可信计算平台 $M(S,O,D,C,R)$，其中，S 为平台主体集合，s 表示单个的主体；O 为平台数据集合；o 表示单个的数据个体，其中包括空个体 ϕ；D 为数据流动的范围，其中 D_m 表示为数据流动的范围在平台内部，$D-D_m$ 则表示数据流动的范围为平台外部；C 为安全级集合，且分为密文集 C_1 和明文集 C_2，即 $C=C_1\cup C_2$，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)；R 包括 $\{\text{Success, Fail}\}$，表示数据流动的状态。Success 表示允许数据流动，Fail 则表示不允许数据流动。

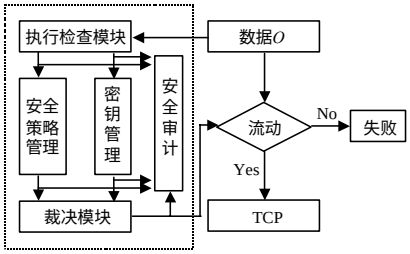
定义 2 M 上的 3 个函数分别为：(1) $f:O\to C$，安全级判定函数，即判定主、客体的安全级别。(2) $\Gamma:(O,D)\times D\to R$，为数据流向判定函数，即判定是否允许数据流动。如 $\Gamma((o,D_m)\times D_m)=\text{Success}$，即平台内部的数据 o 要在平台内部流动，且此次数据流动是允许的。(3) $@:O\to O$，表示数据流动后产生的数据副本。

3 基于 TPM 的终端数据可信迁移模型

基于 TPM 的终端数据可信迁移应该具备下列条件：(1)数据迁移过程必须以密文形式存在，且迁移过程对合法用户应该是透明的。(2)无论在迁出平台或迁入平台，数据相应的保密级别不应降低。(3)只有合法终端及合法用户能够在迁入平台解密迁移的数据。可信迁移模型如图 2 所示。



(a)可信计算平台终端



(b)PMC

图 2 可信迁移模型

图 2(a)是可信迁移模型中平台终端的工作模型图。TPM 是可信计算平台的可信根，负责提供平台终端所需的密码服务。“全程 BLP 规则”是 PMC 下发给终端的安全策略之一，负责平台终端的数据安全操作。“安全审计”负责对终端的各种操作进行安全审计。“执行检查模块”和“裁决模块”负责终端各种安全操作的权限判定。

平台终端首先由“执行检查模块”将待迁入/迁出的数据信息传递到“全程 BLP 规则”模块，由该规则检查数据的迁移权限；“裁决模块”通过 TSS 对 TPM 密码服务的调用完成对终端数据的透明加/解密操作，包括数据的迁移操作等。具体过程见 3.2 节。

图 2(b)是可信迁移模型中 PMC 的工作模型。在此过程中，PMC 起到策略管理中心和密码管理中心的作用。其中，“安全策略管理”负责根据可信计算平台特定的环境安全需求制定相应的安全策略，并将策略转化为安全策略文件，同时负责在数据可信迁移阶段的策略判断。“密钥管理”负责根据各平台终端的需求，为平台定制各种初始密钥，如 EK, SRK 和 PEK。“安全审计”负责对 PMC 操作进行安全审计。“执行检查模块”和“裁决模块”负责在数据可信迁移阶段对迁移数据的迁移权限进行判定。

PMC 对数据可信迁移的检查首先由“执行检查模块”进行，根据“密钥管理”模块提供的密钥由“安全策略管理”模块提供策略检查，最后通过“裁决模块”将数据的迁移权限及密钥信息反馈给平台终端。

3.1 全程 BLP 规则

在可信计算平台终端的整个生存周期里，无论在平台内部、迁移过程中，还是在迁入平台上，敏感数据都有严格的保密性要求，因此，本文提出“全程 BLP 规则”，它不仅是在敏感数据的生存周期内可信计算平台终端数据安全存储、访问的依据，还是决策敏感数据迁移行为的全程控制规则。

在可信计算平台 M 上：

规则 1 内部流动规则

对 $\forall o\in O$，

$$\Gamma((o,D_m)\times D_m)=\begin{cases}\text{Success} & \text{if } \exists o'\in O,@(o)=o'\wedge f(o)\le f(o')\\ \text{Fail} & \text{else}\end{cases} \quad (1)$$

即：若 $\Gamma((o,D_m)\times D_m)=\text{False}$，则 $@(o)=\phi$。

平台内部的敏感数据 o 要在平台内部流动时，必须由低安全级流向高安全级；否则敏感数据会被降低安全级，从而导致敏感数据在平台内部泄露。

本文主要讨论数据在平台之间的迁移，因此，平台内部的流动控制规则不再详细说明。

规则 2 迁出规则

对 $\forall o\in O$，

$$\Gamma((o,D_m)\times(D-D_m))=\text{Success if } \exists o'\in O,@(o)=o'\wedge f(o)=f(o') \quad (2)$$

当平台内部的敏感数据要流出终端时，从方便用户使用的角度考虑允许其流出终端，但必须以密文形式流出，且流出后的安全级别与流出前的安全级别保持一致。

规则 3 迁入规则

对 $\forall o\in O$，

$$\Gamma((o,D-D_m)\times D_m)=\begin{cases}\text{Success} & \text{if } \exists o'\in O,f(s)\ge f(o)\wedge@(o)=o'\wedge f(o)=f(o')\\ \text{Fail} & \text{if } f(s)<f(o)\end{cases} \quad (3)$$

其中，s 表示对客体 o 执行流入操作的主体。平台外部的敏感数据 o 通过介质流入到平台 M 内部时，执行流入操作的主体 s 的安全级必须不低于客体 o 的安全级才允许其执行 o 的

流入操作，否则拒绝。因为若 s 安全级别低，则流入 M 的敏感数据 o 可能会泄露给低级别的主体。

3.2 终端数据可信迁移流程

由上文可知，可信计算平台系统中 PMC 负责安全管理和密码管理。在对平台终端进行安全初始化过程中，PMC 生成各终端的平台加密密钥(Pub/Pri，公钥/私钥)，密钥生成过程参考文献[3-4]。同时 PMC 维护一张信息表(Information List, IL)，每一项内容包括各个终端对应的平台加密密钥的公钥。PMC 用自己的用户密钥(UK)对其加密后保存在 PMC 中，该列表内容不能被外部获知。其中，加密操作由 E 表示；解密操作由 D 表示。

(1)数据迁出

流出平台 M 的客体 o 应满足以下条件：

1)M：由“执行检查模块”根据“全程 BLP 规则”判断待迁出客体 o 是否满足规则 2，若不满足，由“裁决模块”拒绝该次操作，否则执行 2)。

2)M：由“裁决模块”通过 TSS 调用 TPM 命令生成随机的对称密钥 k，并计算 $o_1 = E_k(o)$。

3)M：用本地平台 PEK 私钥对 k 进行加密，得到 $E_{Pri_M}(k)$。

4)M：用 PMC 的 PEK 公钥 Pub_{PMC} 对 $(k \| E_{Pri_M}(k) \| f(o))$ 加密，并得到 $o_2 = Pub_M \| E_{Pub_{PMC}}(k \| E_{Pri_M}(k) \| f(o))$。

5)M：流出的客体为 $o' = o_1 \| o_2$。

此时，客体 o' 以密文形式流出平台 M。

(2)数据迁入

客体 o' 可以流入平台 M'，但平台 M' 的用户能否解密并使用客体 o' 应满足以下条件：

1) M'：通过 TSS 调用 TPM 生成 $nonce$，计算 $o_1' = Pub_{M'} \| E_{Pub_{PMC}}(nonce \| E_{Pri_{M'}}(nonce) \| f(s))$，且将 $o_2' = o_1' | o_2$ 发送到 PMC；其中，$f(s)$ 为平台 M' 上当前执行客体 o 流入操作的主体的安全级别。

2)PMC：通过“密钥管理模块”调用 PEK 私钥对 o_2' 计算可得

$$o_3' = D_{Pri_{PMC}}(o_2') = Pub_{M'} \| nonce \| E_{Pri_{M'}}(nonce) \| f(s) \| Pub_M \| k \| E_{Pri_M}(k) \| f(o)$$

验证 $D_{Pub_{M'}}(E_{Pri_{M'}}(nonce))$ 与 $nonce$ 是否相等，验证 $D_{Pub_M}(E_{Pri_M}(k))$ 与 k 是否相等，若不相等，则说明 o_3' 受到攻击或假冒，由“裁决模块”返回给 M' 失败信息；否则继续。

通过“密钥管理模块”查询 IL 链表中是否存在包含 Pub_M 和 $Pub_{M'}$ 的表项；若存在，则可证明平台 M 和 M' 的合法身份；否则由“裁决模块”返回给 M' 失败信息。

通过“安全管理模块”比较 $f(s)$ 与 $f(o)$ 之间的关系，若 $f(s) < f(o)$，则由式(3)可知“裁决模块”不允许 o' 流入平台 M' 中；否则继续。

计算 $o_4' = E_{Pub_{M'}}(k \| nonce + 1)$，并发送给 M'。

3) M'：脱密 o_4' 得到 $o_5' = D_{Pri_{M'}}(o_4') = (k \| nonce + 1)$；并可根据 $(nonce + 1)$ 的值判断该次交易的完整性，若不完整，则由“裁决模块”返回失败信息，否则计算 $o_5' = D_k(E_k(o)) = o$，最终得到明文 o_5'。

此时，M' 可以对明文 o_5' 进行处理并保存，但必须满足 $f(s) \geq f(o_5') \geq f(o)$。

数据迁入过程如图 3 所示。

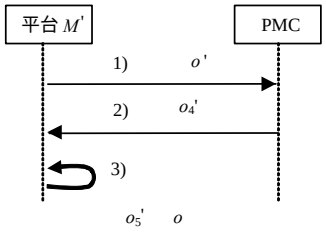


图 3 数据迁入

3.3 安全性分析

(1)密钥安全性

在该模型中，所有的密钥操作和密码服务都由 TPM 提供。由于 TPM 的保护能力(protected capability)和设计原理，同时数据迁入、迁出过程对用户透明，用户不可能从工作流程和 TPM 中得到相关密钥。攻击者在得不到密钥的情况下，解密迁移数据在计算上不可行。

(2)迁移安全性

由 3.2 节可知，数据流入、流出都是由“全程 BLP 规则”决定的。

在数据迁出阶段，首先由“全程 BLP 规则”对待迁移数据进行筛选，符合条件的数据由 TPM 提供的密钥支持以密文形式透明进行，不可能泄露任何敏感信息。

迁入阶段通过对待迁入数据进行检查。可以判定数据的来源以及待迁入平台的身份是否合法。如果待迁入平台或迁出平台不在 PMC 的管辖范围内，就无权进行数据的迁入操作。然后判断当前迁入平台中执行客体 o 流入操作的主体安全级与客体安全级之间的关系，防止低安全级主体访问高安全客体。

由于迁入流程需要平台管理中心参与解密过程，一切恶意代码或非合法迁入数据都无法进入可信计算平台终端。迁入流程可同时防止“假冒”和“中间人攻击”。

(3)操作安全性

在整个数据可信迁移过程中都由“审计模块”对用户的操作进行安全审计，方便系统管理员对各种安全事件进行追踪审计。

4 结束语

该方案主要有以下几个特点：(1)利用 TPM 实现数据迁移的密钥管理问题，便捷、安全；(2)根据“全程访问控制”的思想，在数据迁移过程中保证迁移数据的访问权限；(3)可以保证迁移数据的机密性；(4)可以防止恶意代码通过移动存储设备感染可信计算平台终端。网络上信息迁移过程与通过移动存储设备的迁移过程类似，下一步工作将考虑可信计算平台的网络特点，进一步扩展到网络上的信息可信迁移操作。

参考文献

[1] 国家保密局. 计算机信息系统保密管理暂行规定[Z]. 1998.

[2] NSA. Information Assurance Technical Framework (IATF), V3.0[Z]. 2000-09-20.

[3] TCG. TCG Specification Architecture Overview(Version 1.2)[Z]. (2003-10-20). https://www.trustedcomputinggroup.org.

[4] TCG. TPM Main Part 3 Commands Specification Version 1.2 Revision 62[Z]. (2003-10-10). https://www.trustedcomputinggroup.org.

[5] 陈幼雷, 黄 强, 沈昌祥, 等. 操作系统可信增强框架研究与实现[J]. 计算机工程, 2007, 33(6): 12-14.