第 55 卷 第 1 期
2009 年 2 月

武汉大学学报(理学版)
J. Wuhan Univ. (Nat. Sci. Ed.)

Vol. 55 No. 1
Feb. 2009,022~026

文章编号:1671-8836(2009)01-0022-05

基于移动可信平台模块的通用 PC 机系统可信增强

唐为民[1],高 兰[2],彭双和[1],韩 臻[1],沈昌祥[3†]

(1. 北京交通大学 计算机与信息技术学院,北京 100044;2. 第二炮兵装备研究院,北京 100085;
3. 北京工业大学 计算机学院,北京 100022)

摘 要:为了提高终端安全性能,提出并实现了移动可信平台模块(RTPM)和在其支持下的通用 PC 机系统可信增强架构及原型设计方案. RTPM 通过 USB 接口与计算机平台连接,可接管启动控制权对后续启动的系统进行可信度量. 该架构以 RTPM 为支撑实现完整的系统可信引导,将可信计算机制扩展到操作系统和应用层,在不改变 PC 机硬件结构和通用计算机基本输入输出系统的情况下构建可信计算环境,为终端安全技术手段提供基础支撑,具有很强的实用性.

关 键 词:可信计算;可信平台模块;可移动;安全

中图分类号:TP 309.2 **文献标识码**:A

0 引 言

随着信息技术的发展,信息安全问题日益严峻. 目前,一些重要信息系统仍然大量使用通用 PC 机作为终端设备. 由于通用 PC 机硬件结构的安全机制过于简化,通用的操作系统缺少安全性设计,导致信息系统存在诸多安全问题[1]. 因此,解决信息系统的安全问题必须从终端安全入手[2].

可信计算组织(TCG)提出了可信计算的概念[3]:如果计算机平台从一个初始的"可信根"出发,在每一次计算环境控制权发生转换时,信任关系可以通过传递的方式保持下去不被破坏,那么平台上的计算环境就是可信的. 可信是安全的充分条件,也是安全功能正确实施的基础[4]. 可信机制与安全功能相结合才能达到终端系统的整体安全目标,因此,构建终端的可信计算环境对终端安全具有十分重要的作用.

按照 TCG 规范构建可信计算机平台,需要在计算机主板上嵌入可信平台模块(TPM)[5]作为初始的"可信根",提供密码支持和有保护的存储功能,这种特殊的计算机称为可信计算机. 我国正在制订可信计算标准,可信计算规范和技术还有待完善,可信计算机距全面投入应用还有差距. 因此,研究如何在通用 PC 机上实现可信计算机制,增强终端安全性,更具有实用性和现实意义.

目前,在通用计算机平台上构建可信计算环境主要有 3 种方案:① 虚拟机方案. 用纯软虚拟监控机[6]或"虚拟 TPM"[7]构造可信计算环境;② 第三方验证方案. 引入可信服务器,修改通用计算机的基本输入输出系统(BIOS),由修改的 BIOS 与可信服务器配合实现可信引导[8];③ BIOS 直接可信引导方案. 修改 BIOS,由 BIOS 或 BIOS 调用外接 USB-Key 完成可信度量[9~11]. 第 1 种方案缺少硬件支持,不具备"可信根"性质;第 2 种方案需借助可信第三方验证在线实现可信度量,涉及复杂的信任体系,在现有应用环境下实用性受限;第 3 种方案需要对 BIOS 进行大的改造,由于各厂商 PC 机 BIOS 有较大差异,改造工作量大、可操作性不强. 文献[10,11]设计了操作系统可信启动部分,但信任链建立还不完整,尚未到达应用层. 所以,不需要改造 BIOS,为通用 PC 机建立完整的可信增强框架需要进一步研究.

本文设计了一种具备自启动功能的移动可信平台模块(removable trusted platform module, RTPM),实现了 TCG 规范的主要功能,提出了 RTPM 支持下的通用 PC 机系统可信增强架构,并且给出

收稿日期:2008-04-12 †通讯联系人 E-mail:shenchx@cae.cn
基金项目:国家高技术研究发展计划(863)项目(2007AA012410,2007AA012177);北京交通大学科技基金(2008RC021)资助项目
作者简介:唐为民(1968-),男,博士生,高级工程师,现从事信息安全与密码工程的研究. E-mail:twm68@sina.com

了 RTPM 的设计方案,以及实现 Windows 操作系统可信启动和建立可信环境的控制方法,为在通用 PC 机 Windows 操作系统下建立终端安全环境提供可信支撑.

1　RTPM 的设计与实现

在不改造 BIOS 的情况下,RTPM 实现 TPM 功能要具备 2 个条件:① 在计算机平台启动过程中获得控制权;② 对后续启动系统进行可信度量.

目前,通用 PC 机普遍支持 USB 外部存储设备启动功能,那么,RTPM 可以看作可启动移动存储设备和 TPM 的有机结合体,在启动过程中获取系统控制权并实现可信度量、报告功能. 由于 TPM 模块与智能卡芯片功能类似,RTPM 原型样机设计为可启动移动存储设备与智能卡芯片的结合体.

1.1　RTPM 硬件设计

RTPM 硬件主要由 USB 控制芯片、智能卡芯片和 NAND FLASH 存储器 3 部分组成. RTPM 的硬件逻辑结构如图 1 所示.

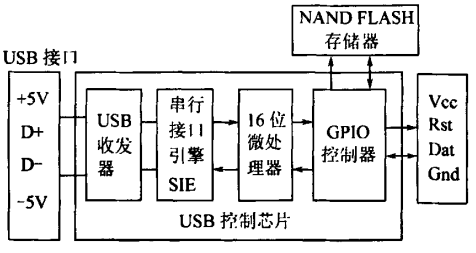

图 1　RTPM 硬件逻辑结构

① USB 控制芯片. RTPM 的主控芯片,它包括 16 位微处理器、USB 收发器、串行接口引擎(SIE)、串行通信接口(SCI)和通用输入输出控制器(GPIO)等部分. USB 收发器和 SIE 与主机进行数据传输(USB2.0 协议)并解析 USB 协议; GPIO 控制器控制 FLASH 存储器实现磁盘读写功能,并控制智能卡芯片完成密码运算功能.

② 智能卡芯片. 密码运算核心硬件,实现 TCG 规范要求的 TPM 密码运算和存储功能.

③ FLASH 存储器. 提供受控存储空间,用于存储启动控制程序和操作系统及应用程序的可信度量预期值.

1.2　RTPM 软件设计

RTPM 软件由 USB 控制器固件程序、智能卡芯片片内操作系统(COS)、启动控制程序 3 部分组成. RTPM 的软件功能结构如图 2 所示.

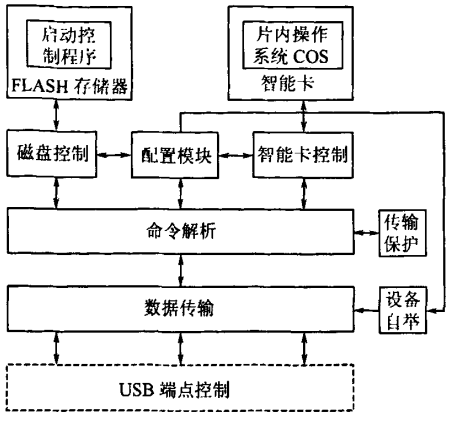

图 2　RTPM 软件功能结构

① USB 控制器固件程序. 由设备自举、数据传输、传输保护、命令解析、磁盘控制、配置模块和智能卡控制等 7 个功能模块组成. 设备自举模块完成 RTPM 的自检、初始化、设备枚举等操作;数据传输模块通过 USB 控制芯片的控制端点、发送端点和接收端点,建立与主机 USB 接口的数据传输通道;传输保护模块使用密码协议在 RTPM 与计算机平台之间形成一条安全通路;命令解析模块负责 UFI 命令解析来区分磁盘操作命令、配置命令和可信机制操作命令;磁盘控制模块实现磁盘读写与 FLASH 存储器读写操作的转换;配置模块实现 RTPM 功能设置和启动控制程序、可信度量预期值写入控制;智能卡控制模块将可信机制操作命令转换为智能卡操作命令和响应,控制 GPIO 控制器与智能卡芯片进行数据通信,完成 TPM 的主要功能.

② 智能卡芯片. COS 控制片内资源实现乱数生成、Hash 计算、ECC 公钥签名以及加密、存储保护和安全控制等功能,COS 与 USB 控制器固件程序按照 ISO7816 协议[12]建立数据交互通路.

③ 启动控制程序. 启动控制程序是能够在通用 PC 机上运行的启动代码,按启动光盘的数据结构存储于 FLASH 存储器中. 启动控制程序接管 BIOS 转来的启动控制权,对 PC 机上的操作系统装载器进行可信度量.

1.3　功能实现

为在移动存储设备的基础上实现 TPM 功能,对 USB Mass Storage 类[13]的 UFI 命令[14]进行扩展,增加配置、配置响应、智能卡操作和操作响应等 4 种命令. 其中,配置和配置响应用于向 RTPM 注入启动控制程序和可信度量预期值,对 RTPM 进行功能配置;智能卡操作和操作响应用于控制智能卡

进行密码运算和受控文件访问,实现可信度量、可信存储和可信报告等功能. RTPM 固件程序解析 Bulk-Only CBW(command block wrapper)封包中的 UFI 命令,分别调用配置模块和智能卡控制模块实现扩展命令功能. 为保证扩展命令传输过程中的安全,在 USB 控制器固件程序和 RTPM 驱动程序中使用密码算法程序和会话密钥协商机制,对所传输的扩展命令进行加密保护.

为了使 RTPM 适应不同厂家的智能卡和密码算法,在 RTPM 接口中封装了可信机制操作命令集(TOCL),可信增强系统与 RTPM 之间传输 TOCL 标准命令与响应,由 RTPM 固件程序实现针对不同厂家智能卡的信息格式转换. FLASH 存储器划分为 3 块:第 1 块以光盘格式存储启动控制程序;第 2 块为 FAT32 格式的移动硬盘空间;第 3 块存储可信度量预期值,由智能卡芯片使用. RTPM 启动时为可启动光盘设备,操作系统加载后转换为普通移动硬盘,由 RTPM 固件程序通过配置命令控制设备类型变换,防止操作系统运行后再次启动 RTPM 的启动控制程序.

2 可信增强系统架构的设计与实现

对通用 PC 机系统进行可信增强的目标有两个:① 使用 RTPM 建立可信计算环境;② 利用可信计算环境为系统安全功能提供支撑,结合其他安全技术实现终端安全的整体目标.

通用 PC 机系统可信增强分为 4 个层次,如图 3 所示. 第 1 层是 RTPM,为在通用 PC 机平台上建立可信计算环境提供硬件基础;第2层是在PC机的

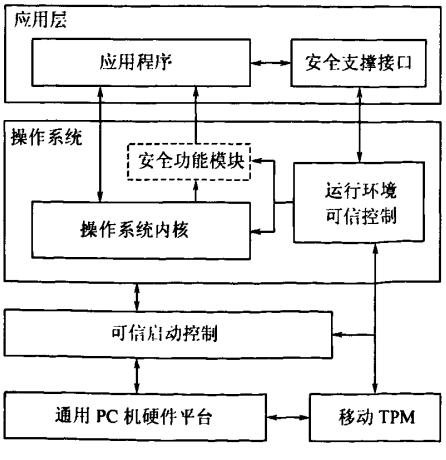

图 3 通用 PC 机系统可信增强总体结构

启动过程中嵌入可信启动控制,对操作系统装载器和操作系统进行可信度量,建立可信操作系统运行环境;第 3 层是在操作系统内核中增加运行环境保护和在应用程序中加载保护控制,提供应用软件可信验证机制,保证应用环境可信;第 4 层是提供应用层安全支撑接口,为其他安全功能提供支撑.

按照上述架构,系统信任传递过程为:BIOS→RTPM→可信操作系统装载器→受保护的操作系统→应用程序.

2.1 可信启动控制

BIOS 完成设备自检后,将 RTPM 作为 USB 可启动光盘设备,加载并运行启动控制程序. 本文通过改造 Grub[15] Stage2 来实现启动控制程序. 启动控制程序的工作步骤包括:① 认证 RTPM 固件程序,协商会话密钥,建立保密通信;② 对用户身份进行认证,提示用户输入智能卡 PIN 码,打开智能卡并启动智能卡的密码运算功能;③ 对 PC 机硬盘内可信操作系统装载器进行可信度量,验证正确后解密可信操作系统装载器并加载到内存中运行.

启动控制程序在实模式下与 RTPM 进行通信,针对普遍使用的 Intel 芯片组 Universal HCI 规范(UHCI)[16]实现了 RTPM 实模式驱动.

2.2 运行环境可信控制

运行环境可信控制的各功能模块与操作系统紧密结合,保护操作系统运行过程中不被篡改;验证并加载运行可信应用程序,保证运行环境可信. 运行环境可信控制主要由可信操作系统装载器、RTPM 保护模式驱动、RTPM 操作接口、操作系统运行保护、应用程序加载保护、安装维护等功能模块组成.

可信操作系统装载器通过改造启动分区 MBR 和操作系统装载器实现. 为防止可信操作系统装载器的可信验证功能被分析、篡改,使用 RTPM 对其进行加密保护,只在运行时解密并加载到内存使用. 可信操作系统装载器对操作系统内核文件(含运行保护模块)及配置文件进行可信度量,验证正确后将控制权转交给操作系统.

将操作系统运行保护模块嵌入到操作系统内核中,对后续的系统服务和核心程序加载过程进行可信度量,保证操作系统环境可信;运用盘写重定向和系统还原技术对操作系统自身进行保护,防止应用程序非法修改操作系统配置;同时为内核层 IPSec 传输加密、文件系统透明加密保护、文件强制访问控制、基于用户的行为监控审计等安全功能模块提供整体保护.

应用程序加载保护模块是安全功能模块的一部

分,它通过系统 API HOOK 技术截获应用程序(含动态链接库)加载过程,对待加载运行的应用程序进行可信度量(根据系统应用环境,可由信息系统的安全管理中心统一生成各终端应用程序的可信度量预期值及可信验证列表,或由用户自己加工并维护应用程序的可信度量预期值及可信验证列表),验证正确后将应用程序加载到内存运行,有效阻止非法应用程序的运行,抵御病毒、木马等恶意代码的攻击.

安装维护模块用于对 RTPM 开机认证和启动控制功能进行配置;对 PC 机可信操作系统装载器代码进行加密保护;对可信操作系统装载器、操作系统及应用程序的可信度量预期值进行计算,并写入 RTPM 保存,以完成针对某一个或群组 PC 机的 RTPM初始化操作.

2.3 安全支撑接口

安全支撑接口主要由管理程序、安全功能接口组成,提供管理、配置 RTPM 图形界面操作接口,调用 RTPM 功能为其他安全功能模块提供支撑.

3 安全性分析

通用 PC 机系统的启动过程如下:① 硬件平台自检. 它包括 PC 机加电,BIOS 运行,检测平台硬件;② 启动引导设备. BIOS 按照 COMS 设置的引导顺序查找可引导设备,将运行控制权交给引导设备;③ 操作系统装载. 引导设备 MBR 开始执行,加载运行特定操作系统的装载程序;④ 加载操作系统. 由操作系统装载程序加载操作系统内核并运行操作系统;⑤ 操作系统加载运行应用程序.

在通用 PC 机上建立可信计算环境必须保证上述各个步骤可信. 在可信平台模块安全性方面,TCG 规范将 TPM 嵌入计算机主板,TPM 设计为标准的片上系统(SOC),未提供物理安全机制保护;而 RTPM 内部的智能卡芯片物理结构具备很好的防物理攻击能力,比 TPM 具有更好的物理安全强度[4]. 在"可信根"构成方面,TCG 规范将 TPM 作为"可信根",可以对 BIOS 进行可信度量,BIOS 被修改后可中断启动过程(安全模式)[3],但并不能防止 BIOS 被修改;本方案将 RTPM 与 BIOS 共同作为"可信根",BIOS 作为 RTPM 运行的基础. 显然,BIOS 的保护和 RTPM 的 USB 通信保护成为本方案"可信根"能否成立的关键,因此,本方案中使用 ROM 芯片或带硬件写保护功能的 FLASH 替代普通 FLASH 存储 BIOS,防止 BIOS 被恶意修改;利用会话密钥协商机制,使用对称密码算法对 RTPM 与 RTPM 驱动程序之间通信的数据进行加密保护,防止关键数据被分析、伪造,保证了 RTPM 的安全. 在 RTPM 的支撑下,信任关系从"可信根"到可信操作系统装载器、操作系统运行保护模块及应用程序加载保护模块逐层传递,从而建立起可信的计算环境. 虽然操作系统运行保护模块通过盘写重定向和系统还原技术,能够防止 Windows 操作系统运行过程中被修改,但是,为保证操作系统的安全性,还需要对操作系统进行合理的配置(包括安装漏洞补丁),防止其自身安全漏洞被利用.

与 TCG 规范相比,RTPM 具备了 TPM 的主要功能,两者具有相同的安全性. 在 PC 机硬件平台和 BIOS 可信的条件下,本文提出的可信增强方案,实现了硬件支持下的完整的系统可信引导过程,并将可信计算机制扩展到了应用层,能够合理地解决为通用 PC 机系统建立可信运行环境的问题,对可信计算体系结构的研究是一种新的尝试.

4 结　论

信息系统的安全要从终端安全入手. 为了使通用 PC 机获得可信计算环境,本文提出了 RTPM 和通用 PC 机系统可信增强的体系架构设计,在不改造 PC 机硬件结构和 BIOS 情况下实现可信增强,为终端安全技术手段提供基础支撑. 在进一步的工作中,将重点进行高速 RTPM 设计、可信恢复方法的研究,提高 RTPM 的性能,使 PC 机可信增强系统具备一定的自我修复能力.

参考文献:

[1] 沈昌祥,张焕国,冯登国,等. 信息安全综述[J]. 中国科学(E辑:信息科学),2007,**37**(2):129-150.
Shen Changxiang, Zhang Huanguo, Feng Dengguo, *et al*. Summarize of Information Security[J]. *Chinese Science(E:Info Sci)*,2007,**37**(2):129-150(Ch).

[2] 沈昌祥. 关于加密信息安全保障体系的思考[J]. 信息安全与通信保密,2004,**41**(5):18-20.
Shen Changxiang. Building an Active and Comprehensive Information Security System[J]. *China Information Security*,2004,**41**(5):18-20(Ch).

[3] Trusted Computing Group. TPM Main Specification: Design Principles V1. 2[EB/OL]. [2008-01-07]. *http://www.trustedcomputinggroup.*

[4] 陈幼雷,黄强,沈昌祥. 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.
Chen Youlei, Huang Qiang, Shen Changxiang. Desig-

ning and Implementing Trusted Enhanced Framework of Operating System[J]. *Journal of Computer Engineering*, 2007, **33**(6): 12-14(Ch).

[5] 张焕国,毋国庆,覃中平,等. 一种新型安全计算机[J]. 武汉大学学报(理学版),2004,**50**(S1):1-6.
Zhang Huanguo, Wu Guoqing, Qin Zhongping, *et al*. A New Type of Secure Computer[J]. *Journal of Wuhan University (Nat Sci Ed)*, 2004, **50**(S1): 1-6(Ch).

[6] Garfinkel T, Pfaff B, Chow J, *et al*. Terra: A Virtual Machine-Based Platform for Trusted Computing[C]// *Proceedings of* 2003 *ACM Symposium on Operating Systems Principles*. New York: ACM Press, 2003: 193-206.

[7] Barham P, Dragovic B, Fraser K, *et al*. Art of Virtualization [C]//*Proceedings of* 2003 *ACM Symposium on Operating System Principles*. New York: ACM Press, 2003: 164-177.

[8] 黄涛,沈昌祥. 一种基于可信服务器的可信引导方案[J]. 武汉大学学报(理学版),2004,**50**(S1):12-14.
Huang Tao, Shen Changxiang. A Trusted Bootstrap Scenario Based Trusted Server[J]. *Journal of Wuhan University (Nat Sci Ed)*, 2004, **50**(S1): 12-14(Ch).

[9] Arbaugh W, Farber D, Smith J. A Secure and Reliable Bootstrap Architecture [C]//*Proceedings of* 1997 *IEEE Symposium on Security and Privacy*. Oakland: IEEE Press, 1997: 65-71.

[10] 任江春,戴葵,王志英. 通用计算机系统的可信增强研究[J]. 华中科技大学学报(自然科学版),2005,**33**:296-299.
Ren Jiangchun, Dai Kui, Wang Zhiying. Research on the Trust Enhancement for General-Purpose Computer [J]. *J Huazhong Univ of Sci & Tech (Nat Sci Ed)*, 2005, **33**: 296-299(Ch).

[11] 陈幼雷,沈昌祥. 可信支撑框架设计及应用模式研究[J]. 计算机工程与应用,2006,**42**(4):16-19.
Chen Youlei, Shen Changxiang. The Trusted Supporting Framework Design and Study of the Application Mode[J]. *Journal of Computer Engineering and Application*, 2006, **42**(4): 16-19(Ch).

[12] International Organization for Standardization. Integrated Circuit Cards with Contacts Part 3: Electronic Signals and Transmission Protocols[EB/OL]. [2007-12-17]. *http://www.cardwerk.com*.

[13] USB Implementers Forum. Universal Serial Bus Mass Storage Class Bulk-Only Transport, Revision 1.0[EB/OL]. [2007-12-17]. *http://www.usb.org*.

[14] USB Implementers Forum. Universal Serial Bus Mass Storage Class UFI Command Specification Revision 1.0[EB/OL]. [2008-01-12]. *http://www.usb.org*.

[15] GNU System. GNU GR and Unified Boot Loader [EB/OL]. [2008-01-12]. *http://www.gnu.org*.

[16] Intel Corporation. Universal Host Controller Interface (UHCI) Design Guide Revision 1.1[EB/OL]. [2008-01-12]. *http://www.intel.com*.

Trust Enhancement of General Personal Computer Based on Removable TPM

TANG Weimin[1], GAO Lan[2], PENG Shuanghe[1], HAN Zhen[1], SHEN Changxiang[3]

(1. College of Computer and Sciences, Beijing Jiaotong University, Beijing 100044, China;
2. Equipment Research Institute of Second Artillery, Beijing 100085, China;
3. College of Computer Sciences, Beijing University of Technology, Beijing 100022, China)

Abstract: In order to enhance the security of terminals computer, this paper presents a design of the Removable Trusted Platform Module (RTPM) and a new architecture of trusted enhancement on general personal computer based on RTPM and its prototype. RTPM that connect with computer through USB can take over the control of booting and validate integrity of following bootstrap process. The architecture can accomplish trusted bootstrap of computer system completely supported by RTPM and broaden the trusted mechanism to operating system and applications. The architecture builds a trusted computing environment on general personal computer without modifying hardware platform and BIOS, can support security module effectively.

Key words: trusted computing; trusted platform module; removable; security