DOI:10.16208/j.issn1000-7024.2011.02.027

可信硬件平台的设计与实现

郭灵儿， 蒋志翔

(中国航天科工集团第二研究院 706 所，北京 100854)

摘 要：针对 TCG 可信平台的核心可信度量根不明确、缺乏有效的端口控制、对外接口速度低等缺陷，设计并实现了一种安全增强的可信硬件平台。该平台在借鉴 TCG 可信平台体系结构的基础上，以可信平台控制模块为核心可信度量根，解决了信任根的保护问题，同时实现了基于身份的 I/O 端口硬件控制，从而具有了更安全的可信启动、I/O 有效控制等优点，可用在对可信安全要求较高的环境中。

关键词：可信计算； 可信平台； 信任根； 可信平台模块； 可信平台控制模块

中图法分类号：TP309 **文献标识码**：A **文章编号**：1000-7024 (2011) 02-0501-04

Design and implementation of hardware platform for trusted computing

GUO Ling-er, JIANG Zhi-xiang

(Institute 706, Second Academy of China Aerospace Science and Industry Corporation, Beijing 100854, China)

Abstract: Aiming at the problems of ambiguous CRTM (core root of trust for measurement), a lack of efficacious control of I/O port, and low speed interface, a security enhanced hardware platform of trusted computing is designed and implemented. Based on the trusted platform of TCG (trusted computing group), this platform sets the trusted platform control module as the CRTM. The security problem of RTM (root of trusted measurement) is solved in this platform. And the hardware control of the I/O ports is implemented based on identity. Therefore, this platform possesses more powerful functions like safer root of trust, efficacious control of I/O, and so on. It can be used in the case which needs more security protection.

Key words: trusted computing; trusted platform; root of trust; TPM; TPCM

0 引 言

随着计算机网络的日益普及，针对计算机系统的病毒木马和黑客攻击也越来越多，手段越来越先进。新型的攻击手段(如 RootKit 等)[1]已经开始针对操作系统内核和 BIOS 等底层系统进行攻击，这些攻击手段隐蔽，难以发现和清除，危害性很大。由于现有计算机体系结构在安全方面的缺陷，传统的防火墙、入侵检测和病毒防护等软件防护手段越来越难以做到真正意义上的安全防护。因此 TCG 组织提出了可信计算这一概念，期望通过结合硬件、BIOS 以及操作系统等底层软件，弥补计算体系结构上的安全缺陷，从整体上提高系统安全。但出于通用性等原因的考虑，TCG 的可信平台存在着一些缺陷，难以满足一些需要使用计算机和网络来处理、传递敏感信息的部门对信息安全更加严格的要求，因此迫切需要一种增强的可信计算平台。安全增强的可信硬件平台在 TCG 可信平台的基础上通过修改 TCG 可信平台体系架构、增加新的模块等方式，弥补了 TCG 可信平台的一些缺陷，可以提供许多新的安全特性，能够满足高可信安全环境的要求。

1 可信计算技术介绍

TCG 组织提出的可信计算的基本思想是：首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，从而把这种信任通过信任链扩展到整个计算机系统，在芯片、主板等硬件结构和 BIOS、操作系统等底层软件进行高级别的防护来阻挡软件层次的攻击，从计算机体系结构上增强系统的安全性。

TCG 的可信平台由可信硬件平台和相关的可信软件构成。可信硬件平台主要由主板、集成在主板上的可信平台模块 TPM(trusted platform module)以及 CPU、存储器等组成。可信平台的核心是 TPM，在 TPM 内部集成了密码部件、非易失性存储器、平台配置寄存器(platform configuration register，PCR)等模块，可以提供签名、杂凑运算、密钥生成、随机数产生、密钥存储、度量信息存储等功能，通过 LPC(low pin count)总线与主板通信[2]。

TCG 认为一个实体的行为在实现给定目标时，其行为总是如同预期一样，那么该实体就是可信的。如果从一个初始

收稿日期：2010-04-26；修订日期：2010-06-27。

作者简介：郭灵儿(1986－)，男，江西遂川人，硕士研究生，研究方向计算机应用技术； 蒋志翔(1969－)，男，四川遂宁人，硕士，研究员，研究方向为嵌入式计算机体系结构及应用技术。E-mail：linger3302@163.com

的信任根出发,在平台环境的每次转换时,这种信任通过传递的方式保持下去(信任链)不被破坏,那么平台环境始终是可信的,运行于其上的各种操作也是可信的,而恶意代码的操作并不是用户所期望的,因此不被信任而不能运行[3]。

TCG 可信 PC 参考架构如图 1 所示[4]。

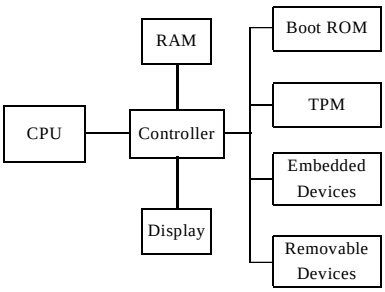

图 1 TCG 可信 PC 参考架构

在可信 PC 中以核心 BIOS(boot block BIOS)作为初始的信任根,即核心可信度量根 CRTM,计算机平台启动时,先加载核心 BIOS,由核心 BIOS 度量其本身和 BIOS 其它模块,如果通过则将控制权交给其它 BIOS,由其它 BIOS 度量去度量下一步要加载的程序,直至将控制权交给操作系统,从而将硬件、BIOS、操作系统等各个部分通过信任链传递联系起来,构建一个可信的运行环境,提供可信度量、可信报告、保护存储、证明等功能。

可信计算思想的提出,推动了对计算机安全的进一步研究,提供了一个计算机安全的解决方向。目前许多计算机厂商和研究机构都在对这个安全机制进行更深入的研究。但是 TCG 在构建可信平台的时候遵循通用、廉价、易用、标准等原则,为适应现有的计算机体系,放弃了一些安全特性,导致这个平台存在着一些缺陷,难以满足高可信安全环境的需求[5]:

(1)在 TCG 可信平台中,可信根由三大信任根组成:可信存储根 RTS、可信报告根 RTR 和可信度量根 RTM。RTM 的初始点是核心可信度量根 CRTM,在 TCG 可信平台,CRTM 并不明确,大多数的实际实现均以 BIOS 的 Boot Block 或整个 BIOS 作为核心可信度量根 CRTM,在其运行之前并不进行完整性验证,而是由其自身保证完整性。由于 CRTM 并未集成到 TPM 中,也就无法受到 TPM 物理上的保护。随着攻击手段的发展,作为连接软件和硬件桥梁的 BIOS 比硬件更容易受到诸如 BIOS Rootkit 等方式的攻击,因而很有可能会被篡改、替换,造成信任根的不可信,导致无法进行度量或度量失效,降低系统的安全性和可信性保障;

(2)为了适用于现有的计算机体系,TPM 通过 LPC 总线挂接到南桥,但是 LPC 总线的数据地址线较少,协议简单,因此容易采集总线上的数据进行分析,降低了模块的安全性;

(3)出于安全考虑,TCG 规范中避免使用对称密钥。对称密钥和非对称密钥各有各的优缺点,需要在应用中互相结合使用才能发挥更好的安全作用。因此不设置对称密钥给实际使用造成了一定的困难。此外 TCG 规范中采用多级树形结构管理密钥,使得对密钥的访问过于繁琐,降低了系统的效率;

(4)在一些高可信安全的应用中,往往希望能在 TPM 中进行高速的加解密运算,但是目前的 TPM 对外的总线 LPC 总线只有 33MHz 频率、4 根地址数据复用线,在该总线上还连接了 Super I/O 等设备,通信速度有限,难以满足高速加解密运算的需求。

为了满足应用中更高的安全需求,有些研究在 TCG 可信平台的基础上,进行了很多改进,如在可信密码模块中提供高速的对称加解密能力、增加对 ECC 的支持、扩展密钥的长度、将 TPM 集成到 Super I/O 中、将 CRTM 整合到 TPM 中[6]等,这些方案一定程度上提高了整个平台的安全性。

2 可信硬件平台的设计

本文在参考 TCG 可信平台尤其是其硬件平台的原理机制基础上结合一些新的技术方法,设计实现了一种安全增强的可信硬件平台。该可信硬件平台由 GM45 主板、安全增强的 BIOS、集成在主板上的可信平台控制模块(trusted platform control module,TPCM)以及 CPU 和存储器等设备组成,其结构如图 2 所示。平台的可信安全核心是由安全控制模块(security control module,SCM)、易失性存储器、非易失性存储器、安全 BIOS 和可信密码芯片等组成的可信平台控制模块(TPCM)。

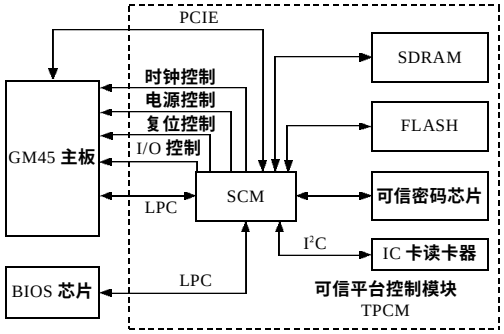

图 2 可信平台硬件系统结构

TPCM 中的 SCM 模块采用 SOPC 方式实现,集成有通过内部 Avalon 总线相连的主板控制模块、密码芯片控制器、FLASH 控制器、SDRAM 控制器、LPC 控制器、PCIE 控制器、I^2C 控制器,并与外部的密码芯片、FLASH 芯片、SDRAM 和 BIOS 芯片互联。可信密码芯片主要完成数字签名、密钥生成、杂凑算法、高速对称加解密运算等功能。易失性存储器为 128MB 的 SDRAM,为 SCM 提供扩展内存。非易失性存储器为 4GB 的 NAND FLASH,用于存储审计日志、BIOS 映像、操作系统内核映像等,并只能由 SCM 平台控制模块访问。在该平台中,可信平台控制模块 TPCM 实现了 TPM 的基本功能,结合其它模块可以实现身份认证、认证启动、I/O 端口物理控制、完整性度量、BIOS 保护和恢复、系统内核恢复、审计日志等多种安全功能。

GM45 主板采用了 Intel 迅驰 2 技术,由 Intel 的 GM45 芯片组和 Penryn 双核 64 位微处理器及相应的外围器件组成,集成有网卡、显卡,提供 PCIE 插槽、PCI 插槽、USB 等接口,具有高性能、低功耗等特点。

2.1 更安全的信任根

在 TCG 的可信平台中,核心可信度量根位于 BIOS 中,无法得到 TPM 的物理保护。在本平台中,根据主板启动过程中各个环节均需要一定的条件,因此形成一个严格的上电时序的情况,设计了一个开机时序控制电路,通过该电路控制主板

启动时序中的重要信号：主板复位信号、南桥电源状态信号和主板时钟开启信号，从而控制住主板的启动，让TPCM先于主板的CPU复位之前启动。在TPCM启动之后，先对BIOS进行度量，然后才释放控制信号，让主板启动。这样就将TPCM作为平台的核心可信度量根CRTM了，从而把可信计算的三大可信根：可信存储根RTS、可信报告根RTR和度量根RTM都集成到了TPCM内部，其安全性和完整性受到TPCM的硬件保护，此外由TPCM控制主板对BIOS的访问，避免了以BIOS或BIOS的Boot Block为CRTM的情况下，可信根可能被篡改替换的缺陷。

安全增强的可信平台的认证启动具体过程如下：

(1)主板的ATX电源加电后可信平台控制模块首先上电，通过控制主板的电源、时钟和复位信号使主板处于复位状态。TPCM读取IC卡信息，判断用户的权限；

(2)如果用户认证通过，TPCM通过LPC总线读取BIOS的内容，并对其进行完整性度量，与之前存储的度量值进行比较，如果校验不一致，则用TPCM中存储的BIOS映像覆盖现有BIOS，完成BIOS恢复；

(3)如果BIOS校验成功，则释放电源、时钟和复位信号，并将GM45主板的LPC总线通过TPCM的内部硬件逻辑连接到BIOS芯片上，此时系统就可以访问BIOS了；

(4) BIOS中的度量代码度量将要加载到内核中的设备驱动程序、MBR和OS Loader；

(5)如果以上度量未通过，就将TPCM中存储的相应映像将其恢复；如果度量通过，则加载这些模块，然后度量操作系统的内核文件。如果操作系统内核度量通过，则开始加载内核，否则也用TPCM中存储的内核映像恢复内核。

以上过程的信任链传递过程如图3所示。

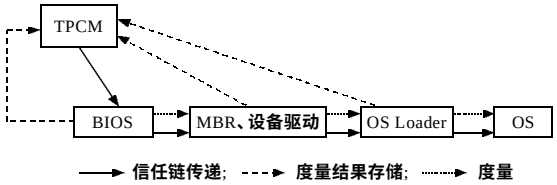

图3 可信硬件平台信任链传递过程

由图3启动过程可见本平台的信任链的传递是以TPCM为度量起始点，先传递到BIOS，然后到MBR、设备驱动，再到OS Loader，最后到OS，一级度量一级，一级认证一级，逐步扩展可信区域，形成一个可信启动的过程，最终建立了一个可信的运行环境。

2.2 基于身份的I/O端口物理控制

在开放式的计算机体系中，并未限制对I/O端口访问，系统中的进程均可访问这些I/O端口。目前对I/O端口所做的访问控制，大都是基于软件方式的，即通过修改I/O端口配置信息中的状态标记来实现的。由于恶意代码与应用程序甚至内核运行在同一个CPU特权级，因此同样可以篡改这些状态标记，从而恶意地打开或关闭这些I/O端口。因此给予软件方式的访问控制很不安全可靠。

通过研究计算机的相关I/O端口，发现每个端口都有一些特殊的控制信号，如时钟信号，选通信号，使能信号等。因此可以使用相应的控制信号线，控制这些信号，从而从硬件上控制这些端口的通断。再结合平台的双因子身份认证机制，通过配置一定的访问控制策略，可以实现按照身份级别来进行I/O端口的控制，做到分级控制管理。

在平台上，可以进行物理控制的I/O端口有：PCI插槽、PCIE插槽、千兆以太网接口、SATA硬盘接口、USB接口、并口、串口、PS/2鼠标键盘接口等。这些端口除SATA硬盘接口外，都可在系统运行的情况关断而不会导致系统崩溃，而且再次开启后可正常使用，利用这一特性，可以与系统的身份认证机制结合起来，动态地管理各I/O端口的使用权限。

2.3 高速加解密运算能力

在TCG可信平台中，出于安全的考虑，尽量避免使用对称密钥，仅使用不对称密钥算法和杂凑算法来实现各个环节的安全防护，这给实际使用造成了一定的困难。因此我国自己制定的《可信计算密码支撑平台功能与接口规范》在可信密码模块中明确地设置了对称加密引擎。在可信密码模块中进行的对称加解密，密钥和加解密过程都不暴露在芯片外，具有较高的安全性，为一些敏感信息的加密存储等提供了有力的保障。由于对称加解密的速度远高于非对称加密，因此需要一条高速的总线来为CPU与可信密码芯片之间的加解密数据提供高速传输通道，而如果采用TCG的TPM模块使用的LPC总线显然很难满足这种高速需求。目前的高速总线一般都是采用串行差分传输技术，如PCI Express*(PCI−E)总线，每个方向的传输速度可达2.5Gb/s，PCI−E x1可提供5Gb/s的双向传输速度。因此在安全增强的可信平台中，采用了PCI−E x1作为加解密数据传输的通道，结合提供高速加解密运算的专用密码模块，可以提供高速的对称加解密运算能力，为可信安全存储提供技术基础。

2.4 BIOS、内核备份恢复功能

新型的软件攻击很多都是针对内核或系统固件，在对这些底层软件系统构建各种防御体系的同时，也必须考虑到被攻击后的恢复问题。目前许多计算机系统采用双BIOS配置来实现BIOS容灾恢复，但这些方法仍然存在许多漏洞和缺陷，如在XCON大会上就曾披露利用Intel公司用于备份恢复的顶层模块交换技术来攻击系统的方法。

因此在安全增强的可信平台中，首先采用大容量NAND Flash存储BIOS、内核以及设备驱动的镜像。其次，将TPCM置于BIOS与主板之间，通过TPCM控制BIOS与主板通信。在系统启动时首先通过TPCM对BIOS进行完整性度量，如果度量确认BIOS遭破坏，则由TPCM将存储的BIOS镜像恢复到BIOS中。相应地，BIOS在度量内核的时候，如果发现内核遭到破坏，也用存储的内核镜像将系统内核进行恢复。

这种BIOS、内核的备份恢复机制，在执行之前都进行了度量和控制，具备较强的抗攻击能力，有力地维护系统的完整性。在远期的应用中，还可以采用多节点备份恢复机制，对BIOS、系统内核、某些特定程序，甚至系统的整个固件、软件系统进行备份恢复。

此外安全增强的可信平台还具有双因子身份认证、审计日志等功能。这些新功能和新特性的增加，大大提高了可信平台在完整性保障、平台控制等方面的能力。

3 测试结果与分析

测试环境由集成了 TPCM 的可信主板及相应的机箱、外设、安全 BIOS 等组成。主要测试可信硬件平台相关功能。测试项目如表 1 所示。测试结果显示，安全增强的可信硬件平台可以实现身份验证、开机时序控制、完整性度量、接口控制、系统恢复和 BIOS 防护等功能。其中完整性度量、身份认证、开机时序控制三者结合可以实现安全的可信启动功能。相对于其它可信平台，本平台以TPCM为核心可信度量根，提高了信任根的安全，在 TCG 的可信平台基础上，还改进增加了身份认证、高速加解密传输通道、审计日志等功能，丰富了可信计算的应用，提高了系统的安全性。

4 结束语

目前，安全增强的可信硬件平台中的 SCM、FLASH、SDRAM、可信密码模块等都作为单独的组件集成到主板上，但在将来可将这些模块通过SoC技术集成到一个芯片中以提高可信平台控制模块的安全性和适应性。

随着人们对计算机信息安全的日益重视，可信计算技术得到产业内的极大关注，研究领域已经由可信 PC，扩展到可信服务器、个人通信、网络接入等多个领域。目前的研究热点也已经由可信平台模块的静态可信深入到动态可信的研究，许多研究针对目前的计算机体系结构和软件结构特点进行了改造和增强以实现动态可信，如 TCG 组织中的核心成员 Intel 正在推进的可信执行技术(trust execution technology，TXT)，通过改造 CPU 和芯片组，添加域管理器创建保护分区等方法来构建可信执行环境。动态可信的实现可以解决信任链传递最后关键一步，实现整个执行环境的可信。可以预见，随着可信计算技术的逐渐成熟，目前困挠人们的计算机安全问题尤其是终端系统的安全将会得到极大的缓解。

参考文献:

[1] 黄校勇，黄小平.Windows Rootkit 技术原理及防御策略[J].微型电脑应用,2006,22(7):4-5.

[2] TCG.TPMsdesign principles V1.2[S].2003.

[3] 刘威鹏,胡俊,方艳湘,等.基于可信计算的终端安全体系结构研究与进展[J].计算机科学,2007,34(10):257-259.

[4] TCG.TCG specification architecture overview revision 1.4[S].2007.

[5] 叶宾.增强可信计算平台模块的可信度[J].信息安全与通信保密,2009(7):53-55.

[6] 张兴,沈昌祥.一种新的可信平台控制模块设计方案[J].武汉大学学报(信息科学版),2008,33(10):1011-1014.

[7] David Challener.可信计算[M].赵波,译.北京:机械工业出版社,2009.

[8] Sean W Smith.可信计算平台:设计与应用[M].冯登国,译.北京:清华大学出版社,2006.

[9] 邓晓军.可信计算的研究与发展[J].计算机安全,2008(2):32-34.

[10] Intel.Intel trusted execution technology architectural overview [Z].2009.

[11] 谭良,周明天.基于可信计算平台的可信引导过程研究[J].计算机应用研究,2008,25(1):232-234.

表 1 可信硬件平台测试用例

基本功能	测试用例	测试结果
用户身份双因子认证	(1) 基于外接 IC 卡对登录用户身份的合法性进行验证；	可以验证
	(2) 基于用户口令对登录用户身份的合法性进行验证；	可以验证
开机时序控制	(3) 主板启动控制；	可以控制
完整性度量	(4) 硬盘、网卡、光驱、声卡和显卡的特征值校验；	可以度量
	(5) PCI 设备特征值校验；	可以度量
	(6) OS Loader 度量值校验；	可以度量
	(7) 可信密码模块设备驱动 (TDD) 度量值校验；	可以度量
	(8) 设备驱动库 (TDDL) 度量值校验；	可以度量
	(9) 可信核心服务 (TCS) 度量值校验；	可以度量
	(10) 操作系统内核文件度量值校验；	可以度量
接口控制	(11) 网络接口控制；	可以控制
	(12) USB 接口控制；	可以控制
	(13) 串口控制；	可以控制
	(14) 并口控制；	可以控制
	(15) SATA 接口控制；	可以控制
	(16) PCI 接口控制；	可以控制
	(17) PCI-E 接口控制；	可以控制
	(18) PS/2 接口控制；	可以控制
系统恢复	(19) 操作系统内核文件数据恢复；	可以恢复
BIOS 自身防护	(20) BIOS 完整性度量；	可以度量
	(21) BIOS 恢复；	可以恢复
	(22) BIOS 防非法篡改；	可以防篡改