第32卷 第24期 计 算 机 工 程 2006年12月
Vol.32 No.24 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)24—0124—02 文献标识码：A 中图分类号：TP309

可信赖计算平台关键技术分析及应用

李春艳
(北京交通大学交通运输学院信息系，北京 100044)

摘 要：基于 TCG 规范的可信赖计算平台是可信计算技术的基础，介绍了可信赖计算平台的发展过程和应用前景，对其关键技术以及可信赖计算平台所具有的重要特性进行分析，并给出具体的应用实例。
关键词：可信计算；可信赖计算平台；密钥；完整性

Analysis of Key Technology in Trusted Computing Platform and Its Application

LI Chunyan
(Department of Information, School of Traffic and Transport, Beijing Jiaotong University, Beijing 100044)

【Abstract】Trusted computing platform(TCP)found on the TCG(trusted computing group) criterion is the base of trusted computing technique. This paper introduces the development of the TCP, and analyses the key technology and main characteristics of the TCP. At last, an instance is given to show the application of TCP.
【Key words】 Trusted computation; Trusted computation platform; Secret key; Integrality

1 概述

由于强调易用性而牺牲了安全性，现有计算机的软硬件结构简化，资源可以任意使用，几乎全部重要的数据和资源都在各种计算机终端里，造成了很多安全隐患。当人们充分享受网络信息技术的成果的同时，也面临着冒充、骗取、入侵等各种计算机犯罪的威胁。如何使人们在“互不谋面”的网络中建立信任，是网络技术发展中必须解决的关键性问题。近年来可信计算技术成为国内外计算机安全技术领域的新研究热点。

可信计算技术是一种针对保护计算机终端的技术，它既可以保护终端内部的资源安全、可靠、不被破坏，又可以在终端之间建立信任关系，构建可信网络。可信计算技术在系统架构上对终端平台进行加固与改造，把不安全因素从终端源头进行控制，旨在把终端建成可信赖的、安全可靠的计算平台，有了它的支持，就可以度量系统的可信性，所以一个可信赖计算平台又是可信计算技术应用的基础[1]。

成立于 2002 年的TCG组织推动了可信计算技术的发展，建立了可信计算平台技术的标准和相应规范[2]，并且不断地地进行完善与改进。TCG提出的可信计算平台技术的基础是可信计算平台模块，简称为TPM[3, 4]。TPM是一个芯片级系统，可以集成在台式机、笔记本、手机和PDA等平台的主板上，通过软件协议栈配合操作系统执行调用命令。它可以生成密钥和使用密钥，进行完整性评估和提供安全存储等，所有这些操作都在TPM内部进行，任何对TPM的访问都要经过授权与严格的认证过程。TPM的诞生将终端的安全保护技术带入了新的阶段。

2 可信赖计算平台的构成

TCG 规范中详细定义了可信赖计算平台的 2 个重要部分，即可信平台模块(TPM)和软件协议栈(TSS)。

2.1 TPM 的构成

可信平台模块的构成如图 1 所示。

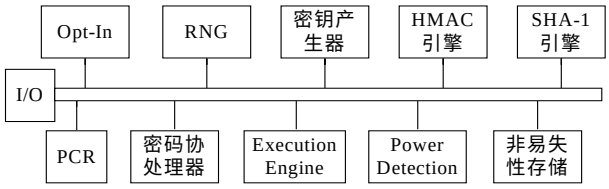

图 1 TPM 的体系结构

(1)I/O 总线：I/O 总线是内外部数据通信的部件。

(2)非易失性存储：用来存储根密钥、用户授权数据及永久性标志。

(3)RNG：随机数发生器是用硬件产生随机数，生成的随机数用于产生密码算法所需的密钥。

(4)SHA-1 引擎：主要使用 SHA-1 算法进行信息摘要运算，输出 160 位的字节串。

(5)密钥产生器：主要用于产生非对称算法的公私钥对和对称算法的密钥。

(6)密码协处理器：主要完成一些基于传统加密算法的操作，这些算法包括 RSA 等非对称算法和 DES 等对称算法，操作包括加密、解密和签名。

(7)PCR：PCR 是一组 160 位的寄存器，用来存放平台完整性信息。

(8)Opt-In：该部件能控制 TPM 的开关、使能、是否激活等；维护 TPM 中永久性和可变的状态标志。

基金项目：北京交通大学人才基金资助项目(2005)
作者简介：李春艳(1975－)，女，博士、讲师，主研方向：信息安全，电子商务
收稿日期：2005-12-21 **E-mail：**lichunyan@jtys.bjtu.edu.cn

(9)Execution Engine：该部件能够执行 TPM 中的相应程序代码，完成相应调用命令的功能。

(10)MAC 引擎：它主要使用 HMAC 算法计算传输数据的 HMAC 值，其中利用的摘要算法是 SHA-1 算法，HMAC 值可检验数据在传输过程中是否被篡改。

(11)Power Detection：该部件负责管理 TPM 的电源状态。

2.2 TSS 的构成

TSS(TCG Software Stack)是可信平台模块和使用 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。

TSS 是一种分层的软件架构，共分 3 层，自下至上分别为 TDDL(TSS Device Driver Library)、TCS(TSS Core Services)和 TSP(TSS Service Providers)，见图 2。

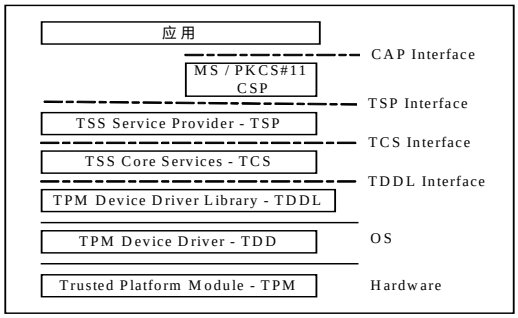

图 2 TSS 的体系结构

TSP 在最上层，提供了丰富的面向对象的应用接口，并且在此可对 TPM 的功能进行扩展，而上层应用程序则必须通过 TSP 来获得 TPM 提供的服务。

TCS 通常以系统服务形式存在，它通过 TDDL 接口层和 TPM 进行通信。同时 TCS 为 TSP 提供接口服务，TSP 是通过调用 TCS 来使用 TPM 的功能。

3 可信赖计算平台的特性

3.1 安全的密码学服务

TPM 中密钥的产生是利用硬件随机数并在芯片内部进行，密钥是以树状方式存储的，即每一密钥都有父密钥，并由父密钥的公钥加密保护。若想访问某一密钥，必须首先得到父密钥，然后用父密钥的私钥解密得到该密钥。TPM 中的所有私钥都不允许在芯片外部使用，从而保证密钥的安全性。

除此之外，任何想使用 TPM 的操作必须是经过授权和认证的，任何不合法的用户都不能使用该 TPM 进行工作。所谓授权是 TPM 拥有者的口令，认证是对由口令和要传输的数据组成的信息流计算得出的 HMAC 值的验证，认证协议包括 OIAP、OSAP、DSAP。

3.2 平台完整性度量

完整性度量是可信赖计算平台的重要特性，是对影响平台完整性的平台特性进行收集和一致性检验的过程。检验的方法是用 SHA1 算法进行散列运算。度量的起点被称为信任根，度量信息的散列值被保存在 TPM 的 PCR 中，通过验证 PCR 中的信息能确定平台完整性是否遭到破坏。每一个可信赖计算平台都存有平台完整性报告。

3.3 唯一的身份识别

每个 TPM 在出厂时都有一个唯一的 RSA 根密钥对，它负责保护所有其它密钥，根密钥一旦生成便不可更改，由于根密钥的不可伪造性和根密钥与 TPM 的一一对应性，因此它可以作为所在可信赖计算平台的唯一身份标识。这一特性极大地增强了平台的可信度，使可信赖计算平台能够作为网上电子交易的主体，杜绝盗用名义的非法行为。

4 可信赖计算平台的应用

“安全启动”是可信赖计算平台的一个重要应用。它的核心思想是保护系统的启动过程，即任何可执行代码和配置数据在执行前必须进行完整性度量。

“安全启动”技术是从系统加电的时刻起，依次对 BIOS、系统 I/O、ROM、硬件、系统内核进行完整性度量，确保系统正常状态启动，并且能对芯片内部存储的密钥、数据以及数字证书提供保护，从而有效阻止病毒、木马、非法程序对系统的攻击和破坏，保证系统免受攻击，可靠、稳定运行。基于可信赖计算平台的安全启动过程如图 3 所示。

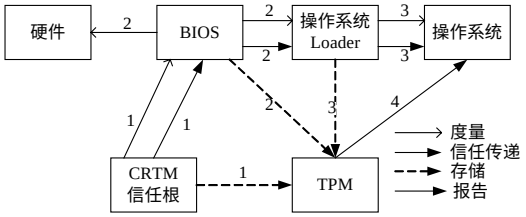

图 3 可信赖计算平台的安全启动过程

具有“安全启动”能力的平台从一个信任的根状态开始启动，该状态成为 CRTM，它的信任是默认的。CRTM 首先度量 BIOS 的信任状态，即收集 BIOS 的特性数据进行散列运算，然后将度量值存入 TPM 中进行验证，如果信任状态是可接受的，则通过“信任传递”将信任边界扩展到 BIOS，再由 BIOS 开始重复上述过程，最后 TPM 将平台完整性报告交给操作系统，由用户判定系统的当前状态。

5 展望

综上所述，基于 TPM 的可信赖计算平台技术是确保终端系统安全与可信的技术，它在保护电子商务、电子交易、预防病毒、蠕虫和其它恶意攻击、数字版权保护等应用中具有重要的价值。

当前，可信计算技术的研究方兴未艾，国外诸多厂商推出了符合 TCG 规范的可信赖计算平台，如 Atmel、Broadcom 和 Infineon 等。国内的联想和兆日也推出了自主研发的安全芯片。可以预见，以可信终端为基础构成的安全计算环境为期不远。

参考文献

1 Trusted Computing Platform Alliance(TCPA). TCPA Main Specification Version 1.1b[EB/OL]. 2002-02. http://www.intel.com/cd/ids/developer/asmo-na/eng/20252.htm.

2 Trusted Computing Group (TCG). TCG Software Stack Specification Version 1.10 [EB/OL]. 2003-08. https://www.trustedcomputinggroup.org/groups/software/TCG Software Stack Specification Version 1.1.pdf.

3 Trusted Computing Group (TCG). TCG Specification Version 1.2 Revision 62. TPM Main Part 1: Design Principles[EB/OL]. 2003-10. https:// www.trustedcomputinggroup org/downloads/tpmwg-mainrev 62 Part1 Design Principles.pdf.

4 Trusted Computing Group(TCG). TCG Specification Version 1.2 Revision 62. TPM Main Part 2: TPM Data Structures[EB/OL]. 2003-10. https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev 62 Part2 TPM Structures.pdf.