第33卷 第15期 计 算 机 工 程 2007年8月
Vol.33 No.15 Computer Engineering August 2007
·安全技术· 文章编号：1000—3428(2007)15—0152—03 文献标识码：A 中图分类号：TP303

一种基于TPM芯片的计算机安全体系结构

邢启江[1,2]，肖 政[3,4]，侯紫峰[3]，姜永华[2]
(1. 山东工商学院计算中心，烟台 264005；2. 海军航空工程学院电子信息工程系，烟台 264001；
3. 中国科学院计算所，北京 100080；4. 中国科学院研究生院，北京 100039)

摘 要：针对现行通用个人计算机基于开放架构、存在诸多攻击点等安全问题，提出了一种基于TPM安全芯片的新型计算机体系结构。设计并实现了基于安全芯片的软件协议栈TSS，在安全芯片中使用软件协议栈，通过核心服务API来调用核心服务模块，解决远程通信的平台信任问题。设计并实现了基于多协议的授权和认证管理，实现上层应用和TPM之间的授权会话及授权认证，从而保证计算机能够完成安全计算和安全存储的工作，使计算平台达到更高的安全性。

关键词：TPM安全芯片；软件协议栈；可信计算；安全体系结构

Computer Security Architecture Based on TPM Chip

XING Qi-jiang[1,2], XIAO Zheng[3,4], HOU Zi-feng[3], JIANG Yong-hua[2]
(1. Computer Center, Shandong Institute of Business and Technology, Yantai 264005;
2. Department of Electronic and Information Engineering, Naval Aeronautical Engineering Institutes, Yantai 264001;
3. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080;
4. Graduate School, Chinese Academy of Science, Beijing 100039)

【Abstract】To solve the problem of computer security, this paper puts forward a new computer architecture based on TPM chip by designing a software protocol stack TSS based on security chip. By using this protocol stack to call kernel service modules through API, the problem of trusted platforms in distance communication can be solved. In the security chip based on TPM, authorization and authentication management based on multi-protocol are designed and implemented to realize authorized communication and authentication between upper application and TPM, ensuring that the computer is able to accomplish the task of safe computation and safe store to enhance the security level of the computing platforms.

【Key words】TPM security chip; software protocol stack; trusted computation; security architecture

1 概述

现行通用个人计算机终端基于开放架构，绝大多数安全机制都以软件形式实现并建立在操作系统之上[1]。而软件形式的安全机制有其固有的安全缺陷，即初始密钥(或根密钥)难以做到高安全性存储，由于现行系统(包括硬件和软件)都以简单口令作为进入系统的钥匙，攻击者可以利用随处可见的黑客工具试出该密钥，冒充合法用户进入系统为所欲为。另外，流行的操作系统(比如Windows)安全级别仅为C2，攻击者能够比较容易地侵入。一旦获得系统控制权，那么由操作系统负责保护的秘密数据、各种系统配置文件就没有安全性可言，在这种环境下运行的应用程序的安全功能不可能真正发挥作用[2]。所以，建立在这样一种操作系统之上的安全机制很难从根本上保障计算平台的安全。

通常讨论安全时都会使用信任假设，上述问题的关键就在于：建立在操作系统之上的安全机制假设操作系统是可信任的或值得信任的，而现行的操作系统本身还不能做到这种程度[3]。这就是现行个人计算机安全问题的尴尬之处。

本文介绍了一种基于TPM安全芯片的新型计算机体系结构。从系统加电开始，到TPM初始化、自检、获取TPM信息，直至启动完毕的整个过程中，系统利用可信赖度量核心根执行一系列度量操作，通过这些度量操作记录计算机平台已经或将要执行的软件的完整性，从而确保整个平台的初始环境是安全可信的。然后提出并设计了基于安全芯片的软件协议栈TSS，通过其提供可靠的安全机制来保证主机能够完成安全计算和安全存储的工作。接着基于TPM的安全芯片，设计并实现了基于多协议的授权和认证管理，成功实现了上层应用实现和TPM之间的授权会话和授权认证。在基于TPM安全芯片的新型计算机体系结构中，由于应用层的各种安全机制的关键部分或最基础部分(密链的根的生成与存储、密码学计算)都建立在安全芯片之上，这样通过安全芯片和上层软件的协同工作就为应用层的各种应用建立了一个可信赖的、安全的计算环境，因此大大提高了系统的各项安全因素水平。根据木桶原理，当系统安全中所有因素的安全水平都提高后，系统整体安全也自然而然地提高了。

2 基于TPM安全芯片的安全计算机体系结构

安全计算机是在原计算机体系结构基础上进行安全体系架构设计而形成的[4,5]，其中，关键部件TPM是一个基于密码

基金项目：国家“863”计划基金资助项目“数字证书SoC芯片”(2004AA1Z1090)；国家“863”计划基金资助项目“可信计算系统平台”(2005AA142030)

作者简介：邢启江(1963－)，男，高级工程师、博士研究生，主研方向：信息安全；肖 政，博士研究生；侯紫峰，博士生导师、研究员；姜永华，博士生导师、教授

收稿日期：2006-08-29 **E-mail：**xingqijiang@163.com

学的安全芯片[6]，通过LPC总线集成在计算机主板上，主板固件BIOS需要重新设计使安全芯片能在系统动态生成过程中对各模块进行信任度量。另外，通过操作系统内核模式的软件协议栈，使安全应用程序以安全芯片为安全基。图 1 描述了基于TPM安全芯片的安全计算机体系结构。

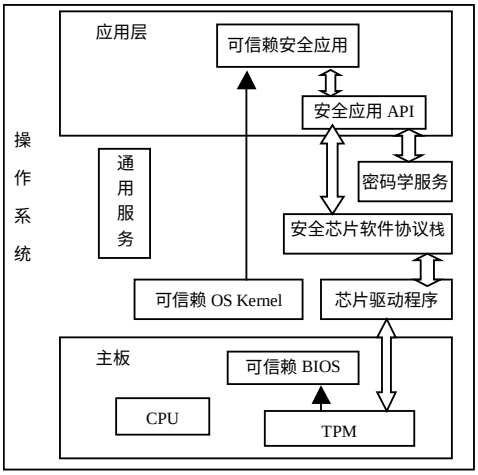

图 1　安全计算机体系结构

3　基于 TPM 安全芯片计算机的实现机制

3.1　安全芯片组成和功能

安全芯片的组成模块如图 2 所示，它具有一系列密码处理功能，包括：安全Hash函数，随机数生成器(RNG)，公钥密码算法密钥对生成器，公钥密码加/解密，数字签名/验证算法，对称密码算法[7]。安全芯片所涉及的密码算法都将采用国家密码管理委员会批准的算法，即国家标准密码算法。

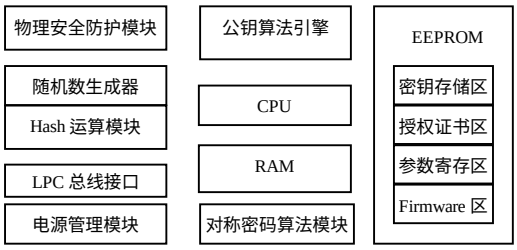

图 2　安全芯片的组成模块

3.2　信任度量——完整性度量与报告机制

安全计算机从一个信赖度量核心根(core root of trust for measurement, CRTM)开始执行一系列度量操作，通过这些度量操作记录着计算机平台已经或将要执行的软件的完整性[8]。大体的过程(图 3)是从开机上电开始监控：BIOS是否是可信任的；由BIOS引导装载的操作系统是否是可信任的；由操作系统加载的应用程序是否是可信任的，同时在操作系统运行过程中可时刻监控关键部件是否被修改。在整个过程中，一旦发现异常立刻发出警报，并终止系统运行，这样，通过该芯片可以使计算平台所有者确信整个平台环境是可信赖的。

基于 TPM 的系统启动过程如下：

(1)调用 Tspi_TPM_SelfTestFull()执行一个完整的自检过程；

(2)调用 Tspi_TPM_GetTestResult()返回自检的结果；

(3)调用 Tspi_TPM_GetCapability()获取 TPM 的信息；

(4)调用 Tspi_TPM_GetRandom()获得 TPM 芯片的 RNG 的随机数值；

(5)调用 Tspi_TPM_StirRandom()给 RNG 增加信息量；

(6)调用 Tspi_TPM_计算机 rExtend()扩展计算机 R 信息；

(7)调用 Tspi_TPM_Quote()获取度量报告。

执行 TPM 芯片加电后的一些硬件初始化工作，完成 TPM 从初始化状态向可操作状态的转换；在 TPM 已经处于可操作状态时，正确执行自检过程；在系统唤醒时，恢复 TPM 的状态；在系统掉电时，保存 TPM 的状态信息；度量结束后，返回相应的度量报告。

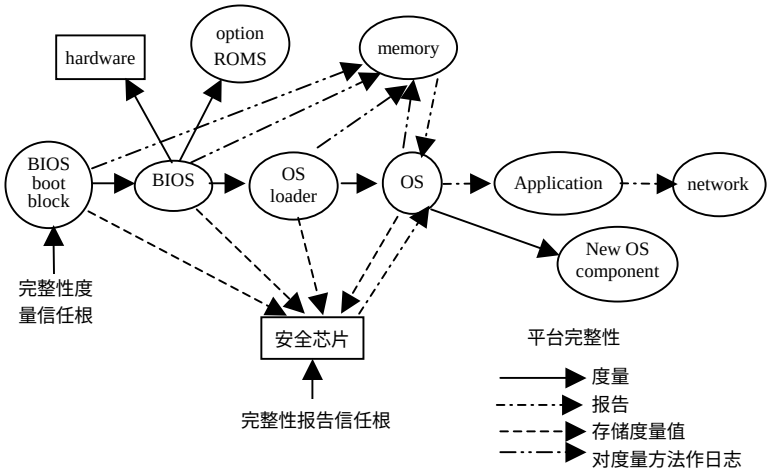

图 3　信任度量示意图

对计算机而言，以 boot block 为 CRTM，由 boot block 度量 BIOS 的完整性并向安全芯片存储度量结果，然后由 BIOS 度量 hardware、option ROM 和 OS loader 并向安全芯片存储度量结果，再由 OS loader 度量 OS kernel 并向安全芯片报告。之后，由安全芯片综合这些度量结果并向 OS 报告 BIOS、hareware、option ROM、OS Loader、OS kernel 的完整性状况，一直延伸下去，一旦某个部件完整性被破坏，系统就不能正常启动，通过这样一个过程，建立了一个信任链关系，由信任链关系来确保计算机平台的可信赖性。另外，计算机平台还可以通过网络向远端平台证明自身的可信赖性，这一特性是电子商务、电子政务最期待的安全特性。

3.3　安全芯片软件协议栈 TSS 机制

安全芯片的廉价性使之便于普及推广，但是其计算和存储资源有限，只用于关键的安全运算和存储，安全计算和安全存储主要还是依靠主机的计算和存储资源来完成，这时就需要可靠的安全机制来保证主机能够完成计算和存储，在基于 TPM 的安全芯片中，该安全机制依靠安全芯片的软件协议栈 TSS 实现。

TSS作为芯片和用户应用之间的平台软件，支持安全芯片向上提供平台认证、密码学服务和芯片管理等重要功能。其内部涉及核心的对象和属性管理、上下文管理、授权与认证、安全操作、密钥管理和TPM管理等模块，是一套非常复杂的平台软件系统[9]。

TSS 采用了分层的设计结构，涉及 kernel 模式(TPM 驱动)和用户模式，最终为上层提供完备的可信计算终端服务。TSS 平台软件从结构上可以分为 3 层，自下至上分别为 TDDL、TCS 和 TSP。TDDL 为安全芯片驱动程序；TCS 为核心服务模块，以内核模式运行，上层向安全芯片的任何功能调用都经由核心服务模块组织安排与控制；TSP 为安全服务提供模块，面向应用层或 CSP/PKCS#11，以用户模式运行，通过核心服务 API 调用来向下传递应用层的安全需求，或将下层的处理结果回传给应用层，其向上也以 API 调用的形式

来提供服务。安全芯片软件协议栈的组织架构如图 4 所示。

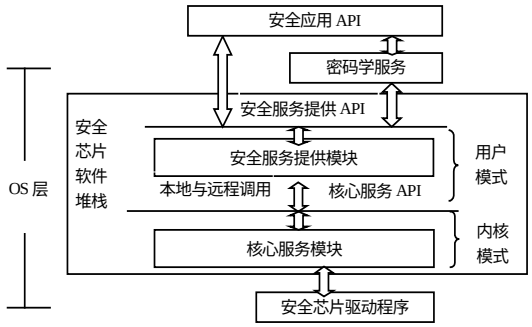

图 4　安全芯片软件协议栈的组织架构

TSS 各部分功能描述如下所示：

(1)安全服务提供模块是用户模式的用户进程，位于 TSS 的最上层，为应用程序提供了丰富的、面向对象的接口，使应用程序可以更加方便地利用安全芯片提供的功能构建需要的安全特性。

(2)安全服务核心模块是用户模式的系统进程，它通过 TDDL 与安全芯片进行通信。除提供安全芯片所具有的所有的原始功能外，还提供更为复杂的功能，比如密钥管理，这涉及到如何对安全芯片中有限的资源进行有效地管理。通过 TCS 的接口，上层应用可以非常直接、简便地使用安全芯片提供的功能。在 TCS 这层软件中，其接口中提供的操作具有原子性。

(3)安全芯片驱动程序提供 2 个功能：1)通过提供标准接口，屏蔽各种不同安全芯片的差异；2)在用户模式和内核模式之间提供一个通信通道。由于用户模式的应用程序无法直接访问内核模式中的程序，因此在这二者之间需要一层软件提供通信支持，该层软件同安全芯片的驱动建立连接后，将独占安全芯片，而且安全芯片的驱动程序不允许 TSS 之外的任何软件对其进行访问。

在安全芯片软件协议栈中，有一个特别功能设计，就是远程进程通过核心服务 API 来调用核心服务模块的功能，其目的是解决远程通信的平台信任问题。通过这项功能，远程的用户可以验证该平台及用户是否为可信赖的，而以前的各种安全解决方案中都没有很好地解决这个问题。

3.4　授权和认证机制

授权和认证模块主要用于工作对象(包括TPM对象、密钥对象和安全操作对象)使用权限的许可和认证通道的安全，使用TPM前时必须进行的授权使用和认证管理。授权通过授权协议的完成，目前TCG主要功能有策略对象管理(TSP层)，对象的授权操作(TCS/TSP)和授权更改(TCS/TSP)[10]。

在基于 TPM 的安全芯片中，设计并实现了基于多协议的授权和认证管理，实现了上层应用和 TPM 之间的授权会话及授权认证。TPM 系统提供 3 个协议将请求者关于授权数据的证明安全地传递给 TPM 芯片：与对象无关的授权协议(object-independent authorization protocol, OIAP)，特定对象的授权协议(object-specific authorization protocol, OSAP)和特定委托授权协议(delegate-specific authorization protocol, DSAP)。其中，OIAP 对任意实体支持多个授权会话；OSAP 对单个实体支持一个认证会话，并能以加密形式传递一个新的授权信息；DSAP 支持所有者或实体授权的委托。授权或授权更改协议的执行需要在 TSP/TCS 和 TPM 芯片进行交互。

图 5 是基于 TPM 的安全芯片中授权和认证操作管理的总体架构。

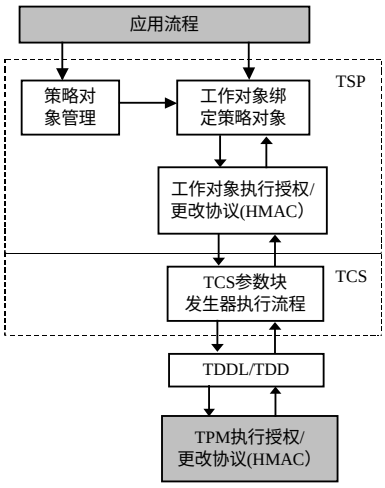

图 5　授权和认证操作管理总体架构

授权和认证操作主要流程描述如下：

(1)相关应用启动授权和认证操作，如 TPM 管理、密钥管理和安全操作等；

(2)应用调用 TSP 完成策略对象的创建和管理，并和某一工作对象绑定，如 TPM 对象和密钥对象等；

(3)TSP 根据上层应用请求开始执行相关授权或授权更改协议，工作对象完成相关计算，如 HMAC 计算，然后调用 TCS 相关接口；

(4)TCS 层利用参数块发生器流化请求，并提交给 TDDL；

(5)TDDL 调用驱动完成相关功能；

(6)TPM 完成相关协议执行，如 HMAC 计算和比较等。

4　结束语

如果 TPM 的安全技术是可信计算的“根”，那么如何有效地管理可谓是其“本”。包括安全模型、密码算法和协议在内的安全技术都与信任相关，都有预先假定的信任前提。因此，如何在网络环境中建立有效的信任关系，如何对这种信任关系进行有效的管理，是目前亟待解决的关键问题，需要进一步的研究。除了个人计算机系统外，这项技术还能够普遍应用于笔记本电脑、掌上电脑、手机等设备。

参考文献

1 陈　钟, 刘　鹏, 刘　欣. 可信计算概论[J]. 信息安全与通信保密, 2003, 24(11): 17-19.

2 侯方勇, 周　进, 王志英, 等. 可信计算研究[J]. 计算机应用研究, 2004, 21(12): 1-4.

3 Arbaugh W A, Farber D J, Smith J M. A Secure and Reliable Bootstrap Architecture[C]//Proc. of 1997 IEEE Symposium on Security and Privacy. 1997-05.

4 郑纬民, 汤志忠. 计算机系统结构[M]. 2 版. 北京: 清华大学出版社, 1998.

5 Carpinelli J D. Computer Systems Organization&Architecture[M]. Pearson Education, Inc., 2002.

6 王新成. 可信计算与系统安全芯片[J]. 计算机安全, 2005, 5(10).

7 曹成来. PKI 安全的关键：CA 的私钥保护[J]. 微计算机信息, 2005, 21(26): 75-77.

8 Trusted Computing Group. Main Specification (Version 1.2)[Z]. 2004.

9 Trusted Computing Group. Trusted Platform Module Protection Profile[Z]. 2004-07.

10 Saltier J H, Schroeder M D. The Protection of Information in Computer Systems[J]. Proceedings of the IEEE, 1975, 63(9): 1278.