TPM安全芯片设计与实现

樊亚军，刘久文
（北京航空航天大学电子信息工程学院，北京 100083）

【摘 要】随着互连网的迅猛发展，对信息安全的要求越来越高，TCG组织提出了基于TPM安全芯片的可信计算平台概念。文章描述了基于TCG规范所设计的TPM安全芯片的体系结构及其核心固件功能模块，包括平台安全信任链的建立、平台身份认证实现及安全权限管理。

【关键词】TCG；TPM；密码；认证
【中图分类号】TP309 【文献标识码】A 【文章编号】1009-8054(2007) 06-0136-02

Design and Implementation of TPM Security Chip

FAN Yajun, LIU Jiuwen
(School of Electronic Information Engineering of BeiHang University, Beijing 100083, China)

【Abstract】Along with the development of Internet, Information Security is becoming more and more important. The Trusted Computing Group established an open specification for an improved computing platform. This paper describes system structure of TPM is explained, based on TCG specification. How to implement the function core of TPM including platform integrity measurement and reporting, platform identity authentication and entities' authorization.

【Keywords】TCG; TPM; Credential; authentication

1 引言

随着互连网的高速发展，像病毒、蠕虫等对信息设备的威胁破坏也在与日俱增，各方面的压力都迫使大家去寻找一种更加基本、应用更加广泛的安全系统来保护数据的私有性和完整性。1999年，可信计算平台联盟(TCPA)宣布成立，它是一个致力于推出跨平台的安全体系结构标准的非赢利性组织，在2003年改组为TCG组织，其提出的可信计算就是涉及到怎样确认一个平台对另一个平台是可信任的，根本目的就是将数据与特定程序、用户或者平台绑定。可信计算平台的核心便是TPM(Trusted Platform Module)安全芯片。

2 TPM安全芯片的体系结构

TPM安全芯片是从体系结构的更底层进行更高级的安全防护，是一种硬件级的安全保护。TPM将敏感数据存放在芯片内部和PC其它组件隔离的存储器内，任何软件攻击方式都是无效的。安全芯片还具备对整个PC系统进行完整性测量的能力，对被黑客软件攻击篡改的PC系统都可以采取必要的自我保护措施。另外，TPM安全芯片中还有相当于身份证的唯一身份识别号，该身份证无法被其他人复制，因而可用于网上身份认证。这些都比传统的以软件为基础附加密钥技术的安全保护来得更加安全可靠。为了从更底层保护计算机系统，TPM必须先于计算机的BIOS和操作系统工作，并且不能使用计算机内存和硬盘等一些容易被外部攻击的公用部件，另外还必须提供一套独立的安全操作中所必备的密码学运算逻辑[1]。该TPM安全芯片内部体系结构如图1所示。

密码学协处理器是该TPM安全芯片中最重要的部件，主要功能模块有：随机数生成器、密钥生成器、SHA引擎、HMAC引擎、对称加密算法引擎和非对称加密算法引擎。随机数生成器负责产生各种运算所需的随机数。密钥生成器负责生成对称密钥和非对称密钥对，对密钥的使用是严格受限的，每个密钥都有其使用范围。SHA引擎负责完成基本的Hash运算，该TPM支持SHA-1和SHA-256，它们的输出

收稿日期：2006-12-18
作者简介：樊亚军，1982年生，在读硕士，主要从事信息安全、嵌入式系统方面的研究。刘久文，1962年生，副教授，主要从事机载数据总线技术、测控技术、嵌入式系统方面的研究。

长度分别是160比特和256比特。HMAC引擎依赖于SHA引擎，用于确认报文数据的正确性，它可以发现数据或者命令流在传输过程中是否发生错误或者被篡改。对称加密算法引擎实现AES、DES运算，出于安全性考虑，它们只供TPM内部使用，不对外提供服务。非对称加密算法引擎实现RSA运算，提供对内对外的数字签名功能，内部存储和传输数据的加解密功能，TCG推荐的密钥长度为2048比特[2]，该TPM可支持512/768/1024/2048比特，其公开密钥取定为：e=0x10001。该CPU是基于51核的单指令周期的8位微处理器，它主要负责解析并通过合理调度资源来执行来自LPC接口的TPM命令流。

NVRAM用于存储每个TPM的唯一身份标识符、TPM敏感状态、密钥和16个PCR(Platform Configure Register，平台配置寄存器)。PCR里面存放的数据是TPM测量得到的当前平台状态单向散列数据。在TCG规范里面并没有特别指定TPM对外的通信接口类型，而是由特定平台决定的，对于PC而言就是采用LPC总线。电源检测部件帮助TPM在平台电源状态发生变化的时候采取适当的措施。

3 TPM安全芯片的特色功能块实现

作为可信计算平台的核心控制部件，TPM安全芯片必须依据TCG规范提供最基本的核心功能块：平台完整性度量和信任链建立；平台身份认证；硬件级密码学运算和密钥保护。

TCG推出的是一种全新的安全系统方案。它从整个平台的基础开始，从系统启动之处开始，在系统的启动过程中会首先执行一个不可打断的整个平台信任链建立序列[3]，它从最低层的硬件开始逐级信任，下一级都会对处于它上面的一级进行完整性检测并向TPM作完整性报告，只有在被确认了安全性以后才可以进一步将信任链往上推。图2演示了系统启动时经过一系列受保护的测量报告动作后建立的信任链，其中Hash Code表示对特定信息块进行单向散列运算，Store Hash表示将先前计算得到的散列值存储到TPM中受保护的PCR寄存器中，Pass Control表示将信任关系传递给下一级，触动下一级开始启动工作，括号中的数字顺序表示信任链建立的次序。TCG规范中采用了两种身份验证方式：基于CA(证书颁发机构)的身份验证和直接匿名身份验证。

基于CA的身份验证实现机制是这样的：每个TPM都有唯一的背书密钥(EK)，它是一对RSA密钥，TPM在第三方信任机构(CA)注册其背书密钥的签名。当验证者需要TPM可信模块证明其可信性时，TPM生成另一对RSA密钥AIK(Attestation Identity Key)，用自己的EK证书证明AIK的公钥代表这个模块可信后将其发送到CA；CA检测到这个EK后认为是可信模块并生成AIK签署证书给TPM；最后TPM将这个AIK签署证书提交给验证方以证明自己的合法身份。

基于CA的身份验证的最大缺点就是每次验证都需要CA的参与，一旦失去了CA的可信性，整个AIK证书和EK之间的关系就都会被泄露。所以在TCG规范1.2版本中提出了直接匿名认证DAA(Direct Anonymous Attestation)，它可以被看成是一个组签名的过程，对于最终的签名没有办法打开但又足以证明对于某个特定RSA公钥该TPM拥有相应的私钥，而且还可以检测出其它非法TPM，这是来自于零知识证明的概念，它可以证明自己是个合法的TPM，但从这个证明过程中外界是不能推出这个TPM的任何私有信息。该TPM便是采用直接匿名身份验证方式。简单来说，首先生成一对用于DAA的RSA密钥对，再生成一对用于身份认证的AIK密钥对；然后用背书密钥EK和DAA私有密钥对AIK公钥进行组签名并将信息发送给验证者；最后验证者根据已知的EK证书和DAA公开密钥对TPM发送过来的信息进行认证及确认其是否为可信任的来源。

硬件级密码学运算和密钥保护主要是依靠独立的密码学协处理器和独立的NVRAM来保障，另外对于TPM的固件来说也有一套严格的软件协议来保障密码学功能模块和密钥的安全使用，这主要涉及权限管理，在该TPM中依赖委托机制和授权协议来达成此目的。

TPM的委托机制是用在想赋予特定实体部分但不是全部所有者权限的情况下。TPM所有者通过创建新的授权值，并委托部分所有者权限给这个新授权值。委托的使用模型是用新授权值代替TPM Owner Token来启动DSAP授权会话。在TPM中靠TPM_DELEGATE表格掌握TPM的委

(下转第140页)

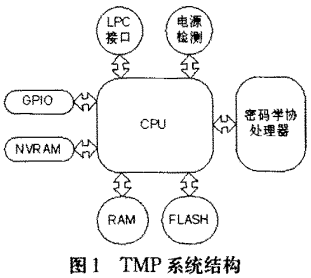

图1 TMP系统结构

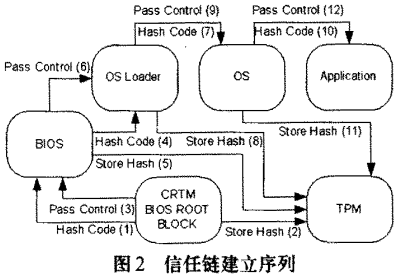

图2 信任链建立序列