可信计算研究进展分析 *

卿斯汉[1,2],周启明[1],杜　虹[3]
(1. 中国科学院软件研究所　北京 100190; 2.北京大学软件与微电子学院　北京 102600;
3. 国家保密科学技术研究所 北京 100044)

摘 要　随着互联网的普及与IT技术的高速发展,可信计算成为热点研究课题。本文分析和总结了可信计算研究的发展现状、体系结构与关键技术,并探讨其发展趋势。最后,提出了我国可信计算标准路线图制定的建议。

关键词　可信计算;可信平台模块;可信密码模块;可信软件堆栈

1　引言

可信计算组织(TCG)由Intel、AMD、微软、IBM、HP等近200家IT公司组成,其使命是开发并倡导开放、厂商中立、跨平台的可信计算构造块及软件接口业界标准规范,其主要技术路线是建立基于硬件的信任根,从基础结构上为可信计算环境的构建提供必要的机制。几年来,TCG倡导的可信计算技术与产品发展迅速,形成了以TPM(可信平台模块)、TSS(可信软件堆栈)、PC平台规范为基础,以包括TNC(可信网络连接)在内的基础设施规范为支撑,辐射服务器、移动电话、存储设备等的标准规范体系。目前正在使用或销售的带有TPM的台式机和笔记本已达数亿台,软硬件厂商推出了众多TCG可信计算技术支撑产品,开源软件的支持为可信计算技术应用软件的开发及可信计算技术的广泛应用提供了可能。同时,学术界也以教学、可信计算技术理论研究方式参与到可信计算技术的发展中。

自TCG组织成立以来,我国从规范及技术角度对基于TPM硬件的可信计算技术进行了深入的分析研究,并于2005年成立了中国可信计算标准工作组。同时,在信息安全及国内主流软硬件厂商的共同努力下,以信息安全相关技术自主可控为目标,推出了使用国产密码算法的TCM(可信密码模块)业界规范及产品,基于TCM的可信计算软硬件产品布局也初成体系,涉及TCM芯片、基于TCM的可信计算机、可信BIOS、TCM驱动及基础软件库、基于TCM的应用软件等。

2　可信计算的技术体系

2.1　TPM与TCM

TPM可信硬件是TCG可信计算技术的核心,其体系结构如图1所示。TPM是可信平台中的关键部件,由受保护的功能及屏蔽的存储位置组成;其基本功能组件包括密码引擎、平台配置寄存PCR、存储器、随机数生成器、执行

*　国家自然科学基金资助项目(No.60970135),国家科技支撑计划资助项目(No.2008BAH33B02)

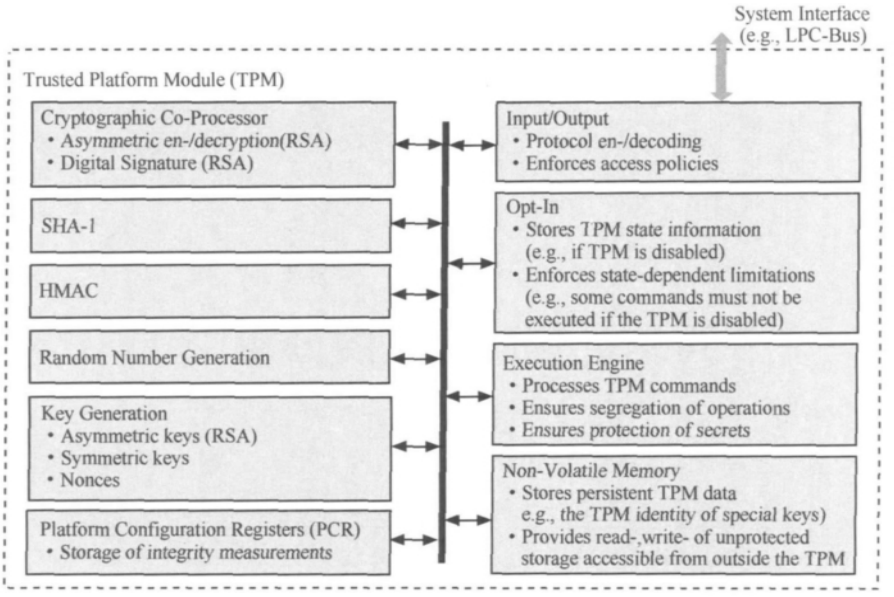

图 1　TPM 可信计算平台模块体系结构

引擎等。TPM 通常作为一个独立组件或其他组件的一部分固定在主板上，并与某个平台进行绑定。

如图 2 所示，TCM 的硬件体系结构与 TPM 类似，其中包含国产分组密码算法 SMS4、国产 Hash 算法 SM3 和国产椭圆曲线算法 SM2。

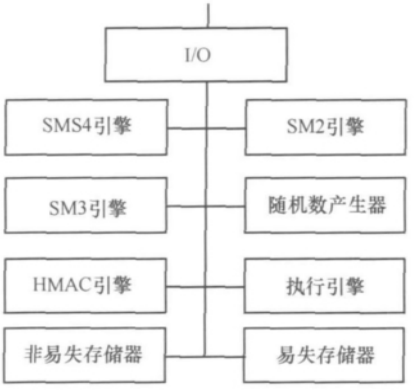

图 2　TCM 可信密码模块体系结构

2.2　可信计算平台核心软硬件体系结构

如图 3 所示，可信计算平台体系结构分为硬件层、内核层、服务层、应用层 4 个层次，具有安全芯片管理接口、安全芯片密码服务接口、完整性管理接口 3 个接口。

硬件层是构建可信计算平台的基础，其中，CRTM（core root of trust for measurements）是平台的信任根，是可信计算平台信任链的源点和起点。内核层直接与 TPM 交互，主要有两个部件：安全密码芯片驱动和安全密码芯片驱动程序库。为了支持不同厂商生产的 TPM 之间的兼容性，在内核层和服务层之间存在安全芯片的管理接口。服务层运行的部件是以操作系统服务的形式存在的，为上层应用程序提供密码管理服务接口，同时具备线程管理的功能。在服务层和应用层之间存在标准的安全芯片密码服务接口。在应用层上，可信计算平台可以利用 TPM 提供的功能支持多种安全服务，如安全芯片管理工具、VPN、安全 E-mail、磁盘加密等。应用层存在完整性管理接口 IMI，该接口提供标准化的安全启动日志管理及完整性服务等操作。

2.3　可信计算基础设施支撑架构

可信计算平台的支撑体系由完整性管理和服务、密钥管理和服务、证书管理和服务 3 部分构成。

（1）完整性管理和服务

在可信计算平台的完整性流程中包含完整性值的创建、完整性度量值的收集、完整性断言创建、完整性评估 4 个阶段。平台的完整性度量和报告受信任根保护，3 个信任根分别为可信度量根 RTM、可信存储根 RTS 和可信报告任根 RTR。通过平台的完整性度量，可信计算平台建立了信任链，信任链的建立必须将 TPM、主机平台、EK 绑定在一起，存在两方面的绑定，即物理绑定和逻辑绑定，物理绑定依赖于硬件技术，逻辑绑定依赖于密码技术。

（2）密钥管理和服务

TPM 在使用过程中会创建大量密钥，密钥分为存储根密钥、存储密钥、加密密钥、签名密钥等类型，按照密钥的迁移性，还分为可迁移密钥和不可迁移密钥。TPM 常见的

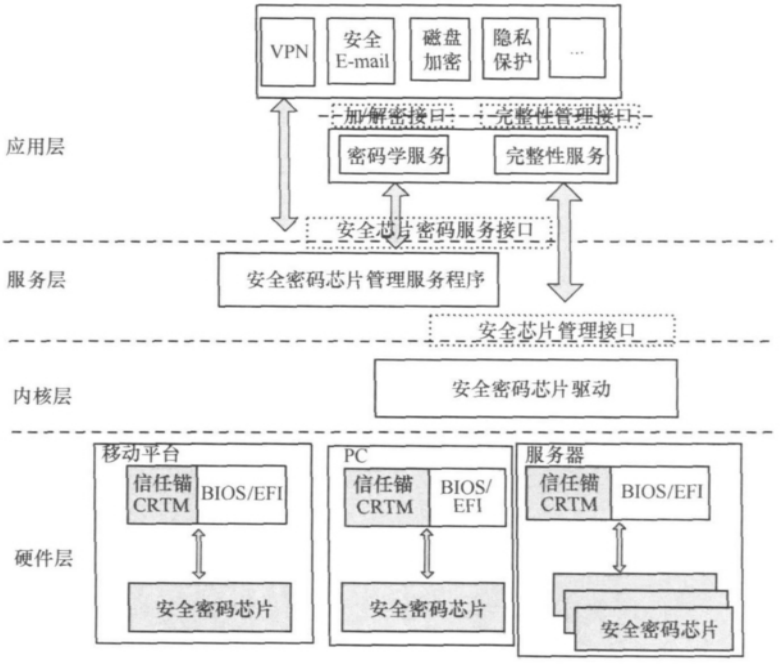

图 3 可信计算平台体系结构

密钥有 EK 密钥、SRK 密钥、AIK 密钥。EK 密钥是平台惟一身份的标识，SRK 密钥是平台存储根密钥，保护其他密钥和数据，AIK 密钥用于证明平台的身份。

(3)证书管理和服务

在 TPM 芯片中，身份信息的标识通过证书完成。证书有两类：一种是 TPM 出厂带有的基本证书，有平台证书、一致性证书、EK 证书，这 3 个证书相互关联，表明 TPM 芯片符合平台要求，有惟一确定的身份；另一种是平台身份证书，由可信第三方发布，标识平台身份，用于证明平台的可信性。最常用的证书有 EK 凭证和 AIK 凭证。

3 可信计算的研究现状与发展趋势

基于 TCG 可信计算技术的发展动态、可信计算业界和学术界的发展动态、我国可信计算的发展动态，可以得出如下结论和预测。

(1)关于 TCG 的可信计算规范

- 以 TPM 可信硬件为核心的规范已经相当成熟，但其可扩展性受到前所未有的挑战，新一代颠覆性的规范 TPM.next 即将问世。
- 在需求驱动下，可信计算平台中可信硬件的集合从单一的可信计算及存储引擎 TPM，向包括可信存储设备在内的多可信硬件扩展，预计不久的将来，类似可信 I/O 设备之类的规范也将加入可信硬件的阵营。
- 可信计算平台规范过去一直以 TPM 作为核心，随着其他可信硬件的加入，对可信硬件的协同管理成为不可忽视的问题，可信平台规范将会对硬件、固件层次的协同管理功能进行规范。
- 与应用部署相关的基础设施规范及可信网络连接规范体系已经比较完善，这部分规范在定义时就注意尽量保持与可信硬件相关部分规范间的独立性。

(2)关于 TCG 的可信计算软件支撑与及应用推广

总地来说，带有 TPM 芯片的 PC 机已经广泛部署，系统软件层次的开源及商业支撑软件已经比较完备，可信计算与传统密码框架之间的适配软件已经相对成熟，但是还存在以下几个问题。

- 除与传统的密码相关的认证、数据保护应用之外，并没有得到其他方面的广泛利用，应用需求有待进一步开发。与可信计算相关的产品、系统的评测工作还不够理想。除 PC 平台之外，包括服务器、移动电话在内的其他设备上的 TPM 产品化及部署情况并不乐观。
- 可信网络连接方面的工作受到广泛认同，但相关工作与 TCG 基于 TPM 的可信平台之间的耦合程度很低，作为可信计算重要组成部分的完整性管理框架的支撑技术尚不成熟。
- 如果 TCG 如期推出下一代 TPM.next 规范，就必须解决不同规范产品之间的兼容性问题。

(3)关于可信计算业界的技术发展

· 在应用层次,可信计算的发展目标仍然是基于可信硬件的,建立必要的软件基础设施,提供对运行环境真实性的认证机制, 提供对系统及数据的机密性、完整性保护机制。

· 从具体的实现机制讲,随着需求及计算模式的不断变化,基于五六年前具体计算平台制订的技术规范的可扩展性已经满足不了现在的需要,适用于虚拟化、云计算环境的新型可信计算支撑机制的研究正在进行之中。

(4)关于可信计算的学术研究

新型计算环境下信任模型的研究,以基于属性的度量为代表的更有效的完整性度量方法研究,现有可信计算技术的缺陷及评估方法研究,可信计算技术的应用模型研究等都是目前较活跃的研究方向。可信计算自产生以来,就与业界、学术界保持着紧密的关系,这也是可信计算技术生命力的来源。

(5)关于我国的可信计算技术发展

· 我国可信计算技术产业近两年取得了长足的发展,成为国际可信计算界一支不可忽视的力量。

· 为了巩固现有成果,当前仍需从技术、产品化、应用推广几个层面大力推动我国可信计算产业的发展,从根本上提高我国可信计算业界的竞争实力。

· 国际范围内的互联互通是不可扭转的趋势,在保证信息安全技术自主可控的前提下,在标准规范层次保证我国标准与国际主流标准的兼容性,才能保证我国标准规范的生命力,保证我国可信计算产业的健康发展。

4 我国可信计算标准路线图的建议

可信计算标准的制定是为了更好地规范我国可信计算技术及产品的研发,满足实际系统的安全需求,保证我国信息安全的自主可控。可信计算标准是面向可信计算产业界的标准,必须注重标准化与产业化的协调发展,产业界的成熟技术形成为标准, 标准反过来对产品的生产、产品在系统中的部署、产品及系统的评估等行为进行规范。相关领域技术的快速发展, 为标准提出了可扩展性的要求,只有能代表新技术、符合客观规律的标准才具有生命力,否则会成为技术发展的阻碍。

我们提出的可信计算标准路线图建议如图 4 所示。路线图分为几个部分,在路线图的中间,是由可信硬件、可信平台、支撑软件、服务软件、可信平台服务接口 5 个层次组成的可信计算规范核心部分;下面是用于可信计算软硬件产品的基础技术规范;左边是参照 CC 标准制定的可信计算各软硬件产品类的保护轮廓规范;右面是可信计算与其他应用基础设施的接口规范。

在可信硬件层次,与 TPM、TCM 规范相对应的是可信计算引擎规范, 与 TCG 存储工作组规范定义相对应的是可信存储组件规范,类似还可根据需要设定可信输入输出组件规范及其他可信硬件规范。

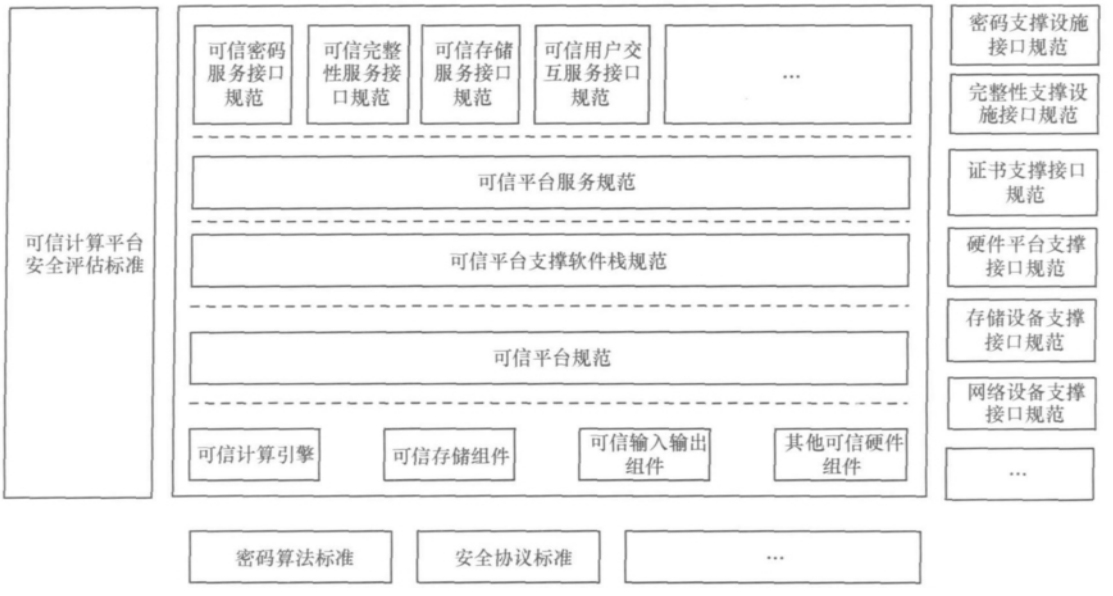

图 4 可信计算标准路线

以可信计算引擎规范为例，它并不是一个单一的规范，而是一个以定义受保护的计算功能及隔离的存储位置为目的的规范集合，集合中包含：一个框架性规范，说明该类可信硬件提供可信支持的基本原理、功能说明、与其他软硬件组件之间的关系等，该规范与平台及密码算法无关；一个通用接口的规范，从抽象角度，定义其与其他组件进行交互的接口；一系列安全子系统的规范，它针对不同应用环境，对框架性规范及接口规范的实例化，这部分规范对应 PC 平台的 TPM 规范、Server 平台的 TPM 规范、移动电话平台的 MTM 规范等，实例规范间可以是并列关系，也可以是继承关系，比如可以实现使用 SHA-1 算法作为 Hash 算法的基于 BIOS 的 PC 平台规范。

安全子系统规范不能与框架性规范及接口规范相违背。

可信平台层次，对应 TCG 的 PC 平台规范，定义可信平台作为一个整体，其硬件、固件提供的可信机制。与 TCG 的可信平台规范不同：为了更好地实现与具体可信硬件、软件的隔离性，在我国规范中，也应该定义一个针对可信平台的框架性规范；可信平台规范的内容不应限于与“可信计算引擎”之间的交互，还应该定义与其他可信硬件之间的交互，作为可信硬件与上层软件进行交互的惟一路径。

- 该层次规范也采用框架性规范、接口规范、安全子系统类的方式定义。以下层次的规范与此类似。
- 可信计算支撑软件栈规范，对应 TCG 的 TSS 规范。
- 可信平台服务规范对可信计算密钥迁移、完整性度量等可信计算具有代表性的专用服务进行规范；可信平台服务接口向外部软件提供与可信平台服务之间的接口。
- 可信计算软、硬件产品的基础技术规范类的设定，是为了支持可信计算规范密码独立性、安全协议独立性等方面的要求，将具体的实现技术从功能规范中独立出来而设定的。
- 可信计算安全评估标准类是可信计算产品评估准则类规范。
- 可信计算与应用基础设施接口规范类是定义可信计算技术与传统应用基础设施之间的接口。

5 结束语

TCG 的可信计算技术受到了广泛关注，我国也推出了使用自主密码算法的 TCM 芯片。作为一种需要各个层次软、硬件相互配合推动的技术，我国的可信计算技术急需标准化来对各参与方的行为进行规范和协调。而如何制定更加科学、更加有生命力的标准规范，如何从标准的角度，在保证相关技术自主可控的同时，保证能够与国际通用技术互联互通，是今后需要重点解决的问题。

参考文献

1 https://www.trustedcomputinggroup.org

2 Ahmad R S. Trusted computing special aspects and challenges. In: SOFSEM'08, Springer LNCS 4910, Germany, 2008

3 国家商用密码管理办公室. 无线局域网产品使用的 SMS4 密码算法, http://www.oscca.gov.cn/UpFile/ 200621016423197990.pdf

4 Sean W. Smith. Trusted computing platforms: design and applications. Springer, USA, 2005

[作者简介] 卿斯汉，研究员，北京大学博士生导师，主要研究方向为信息安全；周启明，副研究员，主要研究方向为信息安全；杜虹，研究员，总工，主要研究方向为信息安全保密。

Progress of Research on Trusted Computing

Qing Sihan[1,2], Zhou Qiming[1], Du Hong[3]

(1. Institute of Software, Chinese Academy of Sciences, Beijing 100190, China;
2.School of Software and Electronics, Peking University, Beijing 102600, China;
3. National Institute of Security Science and Technology, Beijing 100044, China)

Abstract With the popularity of Internet and the rapid development of IT, research on trusted computing is now in the ascendant. In this paper we summarize the state of the art of trusted computing technology, investigate its architecture and key techniques, and analyze its development trend as well. Finally, we suggest a roadmap of trusted computing standard specifications.

Key words trusted computing, trusted platform module, trusted crypto module, trusted software stack (**收稿日期**：2010-12-29)