TPCM 及可信平台主板标准

■ 北京工业大学 / 王冠

为解决计算机关键设备自主可控，推动可信计算产业的发展，增强中国在国际可信计算领域中的话语权，在沈昌祥院士的主导下，展开了中国可信计算机相关标准的研究和制定工作。

可信计算标准族为一个“1+4+4”的格局，其中“1”指的是可信密码，前一个“4”指的是四个主体标准，包括可信平台控制模块（TPCM）、可信平台主板、可信平台基础支撑软件和可信网络连接；后一个“4”指的是四个配套标准，包括可信计算规范体系结构、可信服务器、可信存储和可信计算机可信性测评。整个标准框架构建了以中国密码为基础、以自主可控可信平台控制模块（TPCM）为信任根的可信计算支撑体系。

有关 TPCM 标准的名称为《可信平台控制模块规范》，规定了可信平台控制模块的组成结构、模块内部各个单元的组织管理、可信平台控制模块提供的服务、系统对可信平台控制模块的安全要求、以及可信平台控制模块自身的维护工作。目前该标准完成了国家信息安全标委会的研究和草案稿的编制任务。

可信平台主板标准的正式名称为《可信平台主板功能接口》，规定了可信平台主板的组成结构、信任链构建流程以及功能接口。该标准于 2013 年 11 月 12 日作为国家标准正式发布， 标准文号为 GB/T 29827–2013。

本文介绍可信计算体标准系中 TPCM 和主板两个标准的研制思路以及其中关键问题的解决方案。

1. 标准的创新点

可信计算的核心是信任问题，到底什么是信任的源头至关重要。

国外对可信计算研究比较成熟的是可信计算组（Trusted Computing Group，简称 TCG）。

在 TCG 所提出的方案中，可信芯片为 TPM（可信平台模块），TPM 提供了三个根：可信度量根（RTM）、可信报告根（RTR）和可信存储根（RTS）。

系统启动时，由 BIOS 的 Boot Block 度量 BIOS 的其余部分，BIOS 再对我 OS loader 进行度量，OS Loader 进行度量完以后再对操作系统进行度量，……，完成信任从起点到应用、网络的传递。

TCG 的方案存在 2 个核心问题:

（1）可信度量根在 TPM 保护范围之外，TPM 的一部分代码加上 BIOS 中的一部分代码合起来构成 RTM。因此存在受到攻击的可能性。

（2）信任的起点实际上是 BIOS 的 Boot Block 而不是 TPM，存在被旁路的可能。

基于此现状，我国在标准研制过程中，重点解决以下几个问题：

（1）主动度量与控制。在 TPCM 芯片设计时嵌入 RTM，实现对 BIOS 进行度量的功能，同时，在主板上设计上，通过对主板时序电路的改造，使得 TPCM 成为整个可信平台中第一个获得执行权的部件，实现对其它部件的度量。

使信任源点植入 TPCM 中，实现主动度量与控制，解决了不安全的部件带来的安全问题。

（2）双系统体系结构。在系统加载的时，通过扩展度量代理（EMM），从逻辑上形成两套系统，第一套系统完成传统的计算功能，启动流程还是 CPU、BIOS、OS loader、OS 应用，第二套系统是可信的子系统，通过信任传递，最终

形成信任平台，完成对传统系统的监控。

（3）基于硬件电路的端口控制。利用 TPCM 对计算机资源增设在低于 BIOS 级进行访问控制，增强外设控制强度。

2. 可信平台控制模块规范

2.1 标准研制思路

可信平台控制模块是可信应用的核心控制模块，它为可信应用提供物理上的三个根功能：可信度量根、可信报告根与可信存储根。以可信平台控制模块为基础，可以扩展出可信计算平台的可信度量功能、可信报告功能与可信存储功能。

在研制该标准过程中，重点解决 4 个方面的问题：可信芯片作为可信计算平台的信任源点；实现对密码、证书、私密数据的物理保护；参与建立和保障可信链可信传递；实现对可信平台控制模块的安全调用。

标准从体系结构、固件结构、功能要求、接口协议、封装及引脚和指令接口定义等六个方面对 TPCM 进行了规范。

2.2 TPCM 组成结构

TPCM 的组成结构如图 1 所示。

在 TPCM 内部应包括如下单元：微处理器、非易失性存储单元、易失性存储单元、随机数发生器、密码算法引擎、密钥生成器、定时器、输入输出桥接单元和各种输入输出控制器模块。

非易失性存储单元、易失性存储单元、随机数发生器、密码引擎、密钥生成器和定时器统一映射到片内微处理器的访问地址空间。在地址访问方面，设计者可以自行定义它们在地址空间中的映射关系。

因为要实现对资源访问的控制，需要对身份认证，TPCM 提供身份识别的控制器，连接身份识别

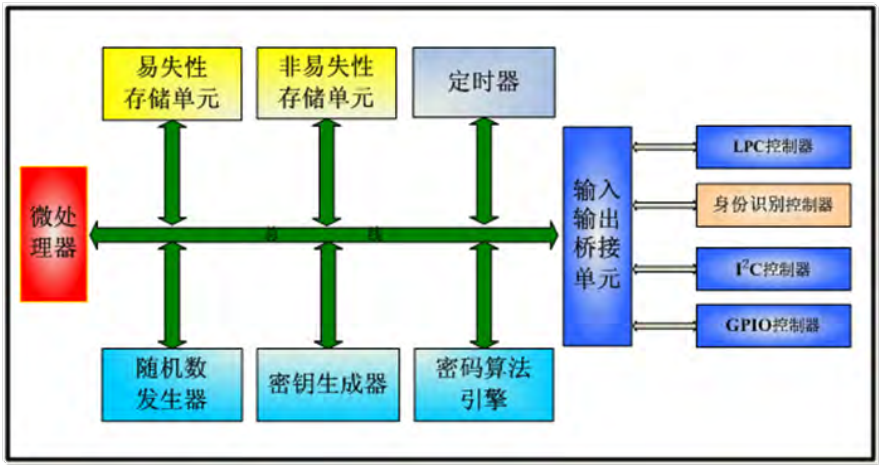

图 1 TPCM 的组成结构

> 我国面临的问题是计算机核心部件不掌握在我们手中，希望利用可信计算芯片成为我们整个安全的一个或者可信的起点，实现对不可信的东西进行监控。

设备。

TPCM 逻辑上是调用 TCM 的功能，实现上可以将密码引擎设计为对 TCM 的调用。

2.3 TPCM 的工作流程

TPCM 在信任链中的工作流程关键点为：

（1）计算平台加电的时保证 TPCM 首先加电，TPCM 加电后进行自检，完成状态检查；

（2）TPCM 读取 BIOS 代码，对 BIOS 进行度量，度量结果存储在 TPCM 中；

（3）TPCM 将控制权交给 CPU，TPCM 变为一个控制设备，为计算过程提供密码服务或者是可信服务。

2.4 可行性分析

（1）TPCM 主动度量的实现。TPCM 支持主、从两种通信方式，主方式就是要完成主动度量，从方式就是一个从设备，接收外部实体的命令。TPCM 的固件中实现对 BIOS 进行主动度量的功能，完成对 BIOS 代码的度量。通过主板外围电路设计，保证 TPCM 首先获得执行。

（2）基于硬件电路的端口控制。TPCM 内部实现用户权限管理表，控制不同用户对平台上的硬件设备的使用权限。提供用户身份识别的硬件实现身份识别；通过 TPCM 对外输出外设控制物理信号实现外设硬件级别的控制。

3. 可信平台主板功能接口

3.1 概述

主板在整个计算机体系中处于一个承上启下的地位，为上层的软件提供运行的平台。为达到可信标准制定的目标，可信平台主板应能实现以 TPCM 为信任根的静态信任链的建立、从开机到操作系统内核加载前的信任链传递。

《可信平台主板功能接口》标准在三个方面对可信平台的主板进行了约束：主板的组成结构，规定 TPCM 与主板的绑定关系、主动度量的实现要求、芯片对外部设备硬件级别的访问控制；信任链构建流程，规定如何进行度量以及度量日志的存储；功能接口定义了主板对外的功能接口，即 BIOS 的功能接口。

3.2 组成结构

可信平台主板是由可信平台控制模块和其它通用部件组成，实现从开机到操作系统内核加载前的平台可信引导功能。通用部件主要包括：中央处理器、随机存取存储器（RAM）、输入输出接口、Boot ROM 固件等。

可信平台主板组成结构如图 2 所示。

相关要求为：

（1）必须确保可信平台主板和 TPCM 一对一的绑定关系。

（2）支持 TPCM 对输入输出接口的控制，TPCM 最少但不限于控制以下输入输出接口的开启或关　闭：USB、PS/2、PCIE、PCI、SATA、串口、并口、网络接口。

（3）在 CPU 执行 Boot ROM 代码前，TPCM 先启动，TPCM 中的 RTM 对 Boot ROM 中的 Boot Block 进行完整性度量和度量结果的存储。

（4）EMM 作为 RTM 度量根的扩展度量模块，实现对执行部件的完整性度量，实现信任链传递。

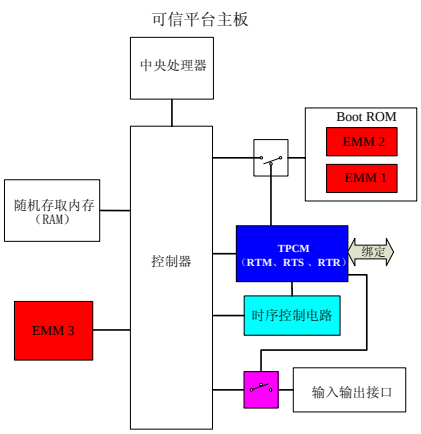

图 2