基于TPCM可信根的双体系可信终端计算架构

黄坚会[1,2,3]，张江江[4]，沈昌祥[1,2]，张建标[1,2]

（1.北京工业大学计算机学院，北京 100124；2.可信计算北京市重点实验室，北京 100124；
3.上海算石科技有限公司，上海 201203；4.山西大学计算机与信息技术学院，山西 太原 030006）

摘　要：冯诺依曼计算机体系由于时代局限性未能考虑到现代的安全环境，计算结构中缺少基于硬件可信根的独立防护部件。基于国家标准GB/T 40650-2021可信平台控制模块（TPCM）可信根的可信终端架构被提出。该架构采用双体系结构实现了基于可信根的渐进式并行可信执行环境架构，从硬件可信根芯片和底层基础软件角度出发解决终端设备源头、平台执行环境及终端设备可信管理的问题。该方法确保终端设备的TPCM可信根芯片和被测基础部件首先上电，完成对CPU执行环境可信度量，并控制CPU电源及设备初始化配置，逐步在计算机启动过程中进行可信扩散。该方法可以在保证设备本体安全可信的基础上实现可靠可信的网络应用，实现设备数据的隐私、安全保障及网络安全。

关键词：国标GB/T 40650-2021；可信根；可信平台控制模块；态度量；可信执行环境

中图分类号：TP393

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2025047

Dual system trusted terminal computing architecture based on TPCM RoT

HUANG Jianhui[1,2,3], ZHANG Jiangjiang[4], SHEN Changxiang[1,2], ZHANG Jianbiao[1,2]

1. School of Computer Science, Beijing University of Technology, Beijing 100124, China
2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China
3. Shanghai Suanshi Technology Co., Ltd., Shanghai 201203, China
4. School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China

Abstract: Due to the limitations of the times, the von Neumann computer system failed to consider the modern security environment, and the computing structure lacked independent protective components based on hardware trusted roots. A trusted terminal architecture based on the Chinese national standard GB/T 40650-2021 trusted platform control module (TPCM) trusted root was proposed. A dual architecture was adopted to implement a progressive parallel trusted execution environment architecture based on trusted roots, solving the problems of terminal device source, platform execution environment, and terminal device trusted management from the perspectives of hardware trusted root chips and underlying basic software. The method ensured that the TPCM trusted root chip of the terminal device and the tested basic components were powered on first, completing the trusted measurement of the CPU execution environment, and controlling the CPU power and device initialization configuration, gradually performing trusted diffusion during the computer startup process. It can achieve reliable and trustworthy network applications while ensuring the security and trustworthiness of the device itself, realizing the privacy, security protection, and network security of device data.

Keywords: Chinese national standard GB/T 40650-2021, RoT, TPCM, dynamic measurement, trusted execution environment

收稿日期：2024–12–31；**修回日期：**2025–03–06

通信作者：张江江, jiang of youth@sxu.edu.cn

基金项目：北京市自然科学基金资助项目（No.M21039）

Foundation Item: The Natural Science Foundation of Beijing Municipality (No.M21039)

0 引言

冯诺依曼计算机体系由于时代局限性未能考虑到现代的安全环境，计算结构中缺少基于硬件可信根（RoT, root of trust）的独立防护部件[1-2]。

目前，大部分网络安全系统处于“被动”防护状态，主要由防火墙、入侵监测和病毒查杀组成的“老三样”占据主体的安全防护地位。“老三样”根据已经发生过的恶意攻击特征库对行为进行对比，从而达到查杀病毒的效果，但是面对层出不穷的恶意攻击方式和未被发现的0-day漏洞，这种被动的防护方式不能很好地应对未知攻击。其次，“老三样”获得了根权限，对用户的访问属于越权访问，而且被恶意攻击者控制，会造成更严重的后果。

可信平台模块（TPM, trusted platform module）[3-5]是由国际可信计算组织（TCG, trusted computing group）提出的安全芯片规范，目前版本为2.0，可以存储和管理密码并提供加密接口。TPM采用外挂式结构，作为外部设备接在系统总线上，而且可信软件栈（TSS, trusted software stack）属于被动调用，无法主动度量。

Challener等[6]指出TPM的所有信任始于CPU BIOS（basic input/output system）中的一段固定或不可变的可信代码。这段受信任的代码测量将要执行的下一段代码，在控制权转移到下一段代码之前，根据测量结果扩展平台配置寄存器。遗憾的是这段被认为固定或不可变的可信代码在现代计算机中也是可变和可修改的。从硬件系统上分析，TPM是受主板CPU计算部件支配的模块，与CPU同步复位，并且由CPU执行的初期一部分代码访问激活并发挥作用。TPM没有控制能力，不具备对源头级别的代码和执行环境进行安全验证，无法很好地防止对处理器、内存和硬盘之类重要部件的篡改替换，无法防御采用已经被篡改的硬件设备来构建伪可信运行环境，无法作为独立、可靠可信的信任源头。《电力物联网可信边缘计算框架关键技术》[7]一文中就明确指出存在可信度量根的核心（CRTM, core root of trust for measurement）在TPM之外，存在易受攻击等难题。

国际上的可信执行环境（TEE, trusted execution environment），通过软硬件方法在中央处理器中构建一个安全区域，其内部加载的程序和数据在机密性和完整性上得到保护。目前主流的TEE技术以X86指令集架构的Inter SGX[8-10]和ARM指令集架构的TrustZone[11-12]为代表。TEE基础原理是将系统的硬件和软件资源划分为2个执行环境，分别为可信执行环境和普通执行环境。这2个执行环境是安全隔离的，有独立的内部数据通路和计算所需存储空间。普通执行环境的应用程序无法访问TEE，即使在TEE内部，多个应用的运行也是相互独立的，不能无授权而互访。TEE可以作为信任扩展过程一个受保护的区域性执行机构，但无法作为信任起点，更不能作为计算单元的可信基础和依靠。

TPM、TrustZone和SGX等[13]硬件安全技术由于缺乏可靠可信根源、主动度量、独立判定和控制能力，没有考虑到计算机运行全过程的可信计算环境保护及动态防护，计算机设备的非法入侵、木马控制等问题没有得到本质性解决。

本文总结现有防护架构技术，发现存在以下问题。

1) 缺乏独立自主可信根。CPU是计算执行单元，受软件的支配和执行环境的影响，且攻击面大，不能作为信任锚点，故无法承担安全可信使命。如果在CPU启动前及启动过程中，固件及执行环境受到了攻击，那么系统平台环境的可信构建则缺乏根基。

2) 执行环境隔离度不够。TrustZone和SGX是在一套CPU体系下的不同物理空间切换，不是彻底的双体系独立环境。TPM是由CPU控制的一个辅助设备，无法脱离CPU计算系统独立存在，也无法提供主动度量和独立可信判定能力。

3) 缺少主动动态度量机制。TPM、TEE和SGX无法主动发起动态度量行为，从而不能对执行代码和执行环境进行实时度量确认和证明。

4) 对计算系统缺少平台系统控制能力。假设现有防护措施能及时发现攻击或篡改，也无法阻止恶性结果的发生或扩大。

我国自主研发的可信平台控制模块（TPCM, trusted platform control module）[14-15]技术提供从加电启动开始进行度量的能力，将BIOS纳入度量对象中，真正可以实现在源头可信基础上的可信任链的建立和传递。TPCM是计算节点的防护部件，可以采用多种技术实现，包括板卡、芯片、IP核等。它的内部包括中央处理器、存储器等硬件和固件，

以及操作系统与可信功能组件等软件，支撑其作为一个独立于计算部件的防护部件组件，并行于计算部件按内置防护策略工作，对计算部件的硬件、固件及软件等需防护的资源进行可信监控和控制，是可信计算节点中的可信根。

本文在研究计算机体系结构和可信根技术的基础上，提出了基于双体系思想[16-17]的可信终端架构，通过渐进式可信扩展，构造具有独立可信度量和防护能力的终端平台系统。该架构综合了广义计算机的全生命周期三阶防护思想[18-19]和广义可信执行环境技术[20]，完善了平台设备从待机、启动、运行直到终端设备关机移除电源的全过程的安全可信。此架构采用国家标准GB/T 40650-2021[15]定义的可信平台控制模块作为信任硬件根源对终端设备系统整个运行过程安全进行保护。本文的贡献可概括如下。

1) 采用双体系结构，使平台的（计算）功能和防护功能分离，通过独立防御单元对（计算）功能进行保障，而且事后可以通过独立可信根芯片追溯存证。

2) 基于TPCM国家标准进行平台系统整体架构设计，解决TPCM的上电时序和系统控制问题。

3) 基于电源系统结构和物理信道设计在计算机运行全过程为TPCM提供计算单元的度量和总线控制能力。

4) 该架构适用于广义计算平台，包括但不限于X86、ARM、MIPS等。

5) 实现对（计算）功能平台全生命周期的主动动态防御。

1　安全可信终端平台防护架构

1.1　可信平台控制模块简介

2022年5月1日，国家标准化管理委员会正式审核通过TPCM国家标准[15]并发布。其中，TPCM基本组成如图1所示。TPCM防御系统如图2所示。从图2中可以看出，TPCM要求先于主机计算部件上电启动，并全程并行于计算部件运行，实现从计算部件第一条指令开始的可信建立。不但在系统启动过程中能防止使用经篡改的计算部件构建运行环境和抵御恶意代码攻击，而且在系统运行过程中能动态地保护运行环境及应用程序的可信安全，最终实现对计算系统全生命周期的可信度量和可信控制。

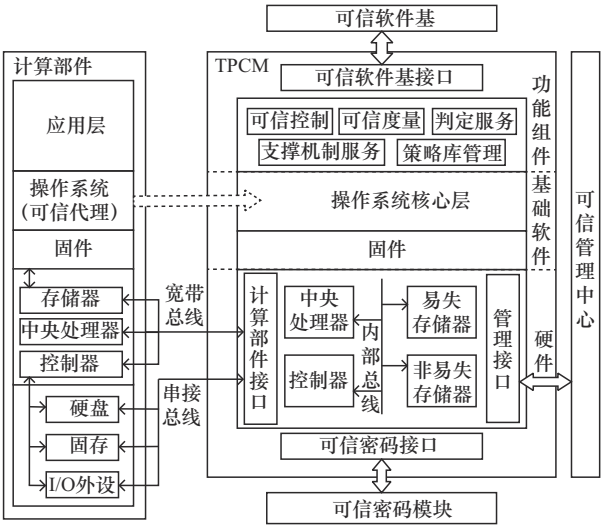


图1　TPCM基本组成

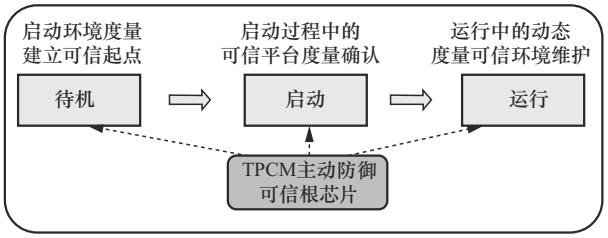


图2　TPCM防御系统

本文所采用的TPCM可信根都已经内置TCM可信密码[21]功能，这样既可以避免TPCM和TCM间的安全通信外露，又可以节省设备的布局空间和功耗。

1.2　可信终端设计思路

以数据采集单元为例，说明终端的运行过程。依照计算机三阶段过程可知，终端从上电到应用可分为：1) 接上电源后终端待机等待开机；2) 当开机信号打开主供电系统，主CPU和外围设备进行初始化工作；3) 当执行环境准备好后，加载应用程序进行数据采集和网络通信工作。

相应地，终端从系统的启动到应用需要待机、启动和运行3个阶段。在这3个阶段中都需要对应防护。1) 待机阶段。对启动代码和CPU指令执行环境的度量确认；2) 启动阶段。可信平台度量确认，操作系统及应用软件执行环境的建立；3) 运行阶段。可信平台的维护，动态监控重要数据、程序代码及执行环境的安全可信。

定义1　基于TPCM可信根，采用双体系结构设计，以广义计算系统的全生命周期为依据，实现对终端执行环境的静态和动态监测防护架构称为双

体系终端安全可信平台架构，简称双体系可信终端架构，如图3所示。

图3右半部分为传统终端计算及控制单元的基本组成，包括片上系统（SoC, system on chip）、电源模块、RTC、EMMC（embedded multi media card）存储、通信端口等，其中SoC集成了处理器、缓存、内存和输入/输出（I/O）等。图3左半部分为TPCM可信根组成，包括时序及可信控制模块、SPI、I2C、EMMC等主控部件。通过对电源时序控制，在CPU上电前发起对CPU计算组件的度量和分析判定以及可信控制输出。SPI通信模块用于计算单元启动过程中对平台组件的度量通信，并由可信控制模块进行控制输出。植入计算启动代码的可信代理程序通过该SPI通信模块响应对平台组件及操作系统程序等信息的采集，并回传给TPCM进行分析判定和可信控制输出。USB高速通信模块用于对内存和计算机执行环境的动态度量功能，结合可信控制模块进行可信控制输出。

根据可信终端架构设计的终端平台，能够以低安装成本和硬件成本的方式建立终端自身执行环境的安全可信，并能快速生成网络身份唯一标识。该思路可以降低底层启动代码和执行环境被恶意篡改可能性。在网络认证和工作过程中，以TPCM作为可信根芯片动态生成平台唯一识别标识及对平台动态度量保护，保障通信网络的准入和工作全过程的安全可信。

1.3　架构设计

1.3.1　*启动代码及环境的主动度量*

TPCM首先上电，主导终端电源控制系统，度量确认启动代码及SoC执行环境的可信性和完整性。如果发现启动代码、配置参数、RTC、4/5G通信模块等环境或固件被篡改替换，则启动安全防范策略，阻止平台上电，或在安全策略控制下进入非可信执行环境，由TPCM通过远程或本地进行设备代码环境重构等。

1.3.2　*平台部件的启动保护*

当终端在启动环境可信的前提下受控启动时，通过在启动代码中植入驱动和保护策略对设备平台执行环境进行检查确认[22]。其中包括但不限于CPU特征、存储特征、外接设备、所有带入平台的固件程序及操作系统。在计算机启动的后期，可以在保证加载代码及内核的完整可信基础上，加载可信操作系统。

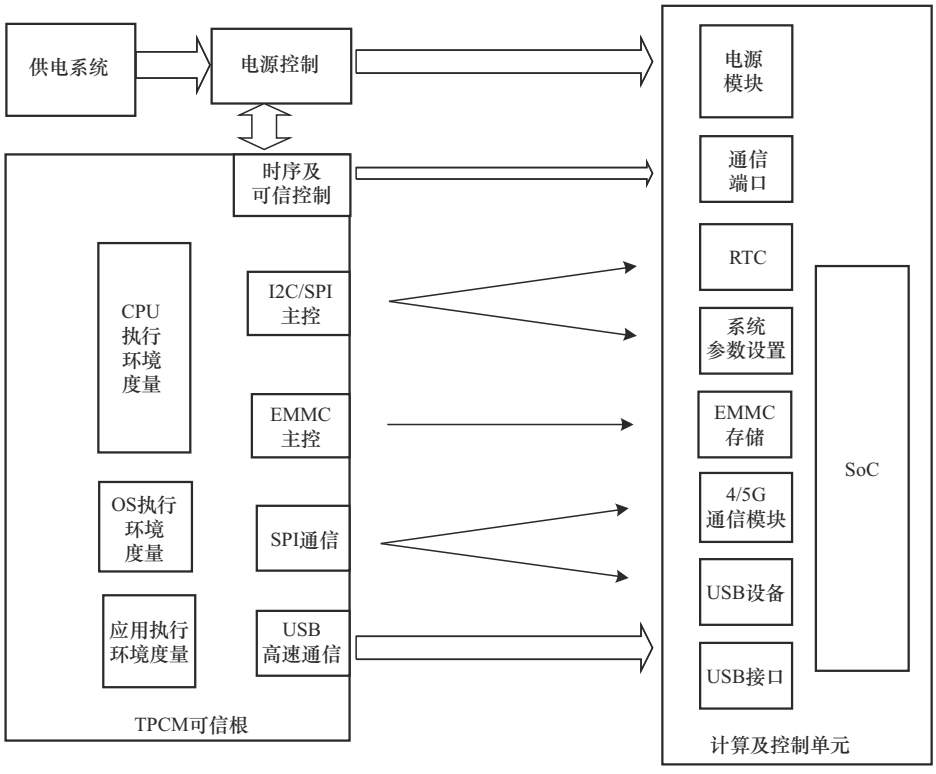


图3　双体系可信终端架构

1.3.3　计算机动态运行环境的监测

系统软件或核心应用软件在被加载和执行过程中，由操作系统可信代理配合TPCM静态和动态防御模块，通过高速总线动态监测内存的数据和代码，并根据保护策略进行管控[23]。

终端设备在与外界建立通信的过程中，通过设备物理特征和通信行为对接入设备进行监管，配合物理通道控制，实现可信运行环境的实时保护。

1.3.4　端口物理控制

终端设备对外的通信物理通道权限被TPCM命令配置成为用户信息并存储于TPCM，由TPCM完成物理信道的自主隔离控制管理。通过作为可信根的TPCM系统来综合评估可信环境后，设置用户对物理端口的访问权项。

TPCM的平台环境功能还可被配置为通过将用户绑定的硬件配置信息与所收集的平台信息相比较来判断该用户是否有权访问本计算机平台或者是否有权进入本计算机平台的可信工作模式。通过该功能可以可靠地管理用户的访问权项。

1.4　平台可信构建流程

TPCM可信根先于主机计算部件上电启动，并且全程并行于计算部件运行，依次完成待机主动度量控制和启动过程的平台度量控制，最后保持运行阶段的动态环境度量防护直至系统关机下电，终端可信防护流程如图4所示。

1.5　基于TPCM的双体系可信平台架构优势

TPM是目前应用最为广泛的可信模块，由国际可信计算组织制定标准[3-4]，在可信计算领域具有代表性。2018年，美国国家标准与技术研究所（NIST）发布NIST SP 800 193标准，被称为平台固件恢复（PFR, platform firmware resilience）。采用基于硬件解决方案保护固件，防止对计算机固件的攻击。它可以理解为国际上为了弥补TPM在第一阶段固件保护的缺少提出了PFR的增强保护措施。故为了体现TPCM的防御优势，本文用TPM加上PFR共同组成可信根，与基于主动防御的TPCM可信根的可信终端平台进行防御功能对比分析，如表1所示。

通过比较总结如下。首先，PFR功能需要一颗独立芯片或包含可信根的现场可编程门阵列（FPGA, field programmable gate array）来完成，而TPM是另外一颗独立芯片，如果结合两者进行可信平台架构设计需要更高的成本、功耗和设计面积代价。其次，由于TPCM是一颗芯片进行计算平台的全生命周期防护，从安全的严密性和延续性来说都优于TPM+PFR平台方案。最后，从表3也表明基于TPCM的平台防御功能整体效果要优于TPM+PFR。综上所述，基于TPCM可信根的双体系可信平台架构作为终端设备安全防护手段是目前比较好的选择。

表1　TPCM与TPM防御功能比较

防御阶段	防御功能	TPCM	TPM+FPR
第一阶段	BIOS/固件代码入侵	摘要比对实时发现，及时更正，警告和/或终止启动	PFR通过签名验签实时发现，及时更正，可终止启动
	实时钟RTC攻击篡改	实时发现，警告和/或终止启动	未有涉及
	启动配置信息修改	实时发现并保护	未有涉及
第二阶段	4G/5G通信模块替换攻击	实时发现，及时警告并终止启动	未有涉及
	BIOS/固件代码入侵	第一阶段已经完成度量验证保护	TPM对主代码进行摘要记录，不进行自主比较和控制
	感染操作系统内核文件	实时发现，及时警告并阻止操作系统加载	TPM通过摘要进行记录，不进行自主比较和控制
	网络等硬件组件篡改或替换	实时发现，及时隔离，警告和/或终止启动	未有涉及
第三阶段	未经认证USB设备	实时发现，及时警告并物理断开USB连接	未有涉及
	木马控制，肆意操控设备	及时警告并剥夺控制权	未有涉及
	内存代码/数据篡改	实时发现，及时警告并报告或控制计算机	未有涉及
	度量报告内容伪造	无法伪造，由TPCM可信根并行进行自主记录存证	CPU操作结果存于TPM，只要早期控制CPU即可伪造

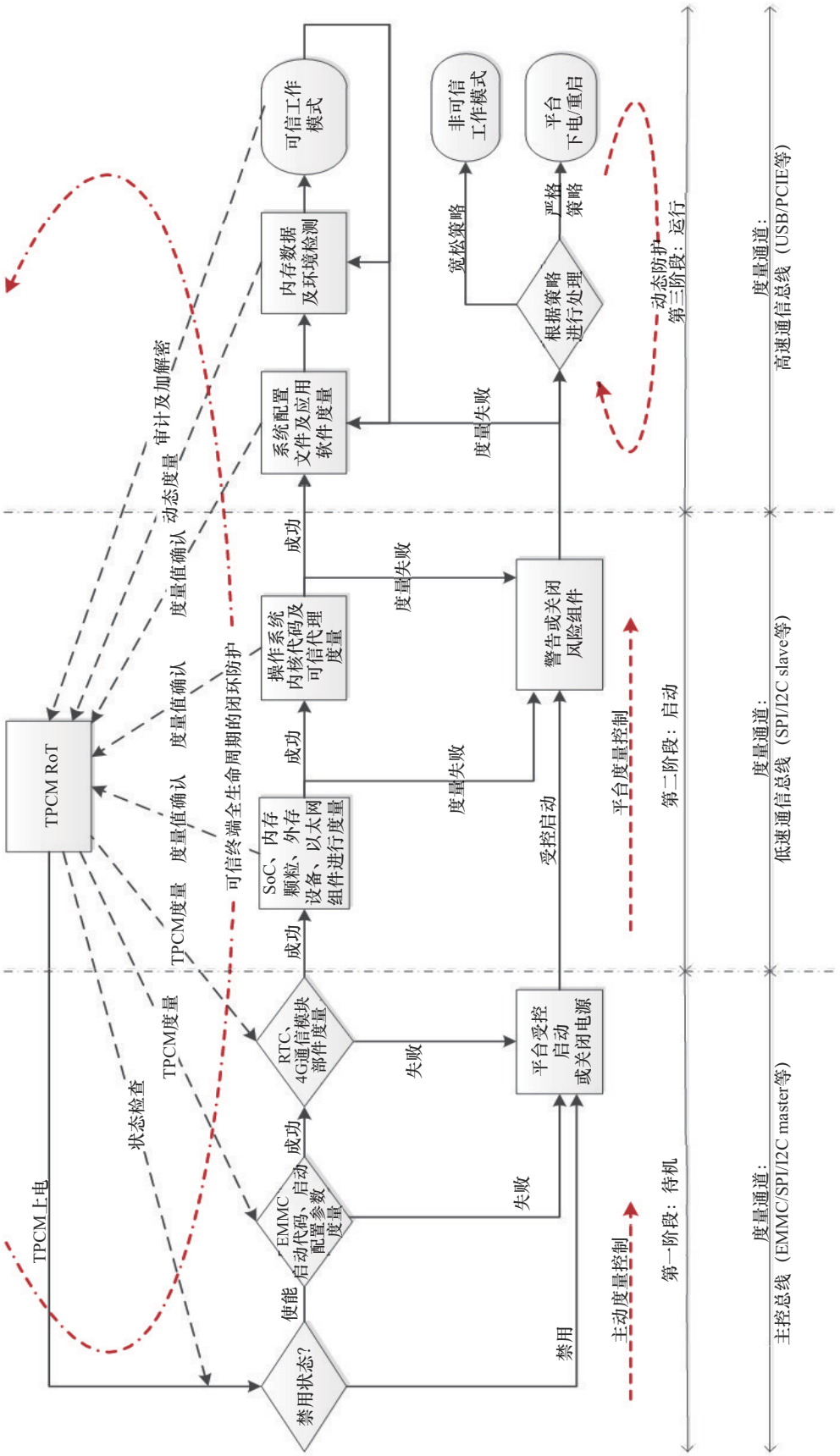

TPCM RoT
TPCM上电
状态检查
TPCM度量
TPCM度量
度量值确认
度量值确认
度量值确认
审计及加解密
动态度量
可信终端全生命周期的闭环防护
禁用状态?
使能
禁用
EMMC
启动代码、启动
配置参数
度量
成功
失败
RTC、
4G通信模块
部件度量
成功
失败
SoC、内存
颗粒、外存
设备、以太网
组件进行度量
成功
度量失败
操作系统
内核代码及
可信代理
度量
成功
度量失败
平台受控
启动
或关闭电源
受控启动
警告或关闭
风险组件
系统配置
文件及应用
软件度量
内存数据
及环境检测
可信工作
模式
根据策略
进行处理
宽松策略
严格
策略
非可信
工作模式
平台
下电/重启
度量失败
主动度量控制
平台度量控制
动态防护
第一阶段：待机
第二阶段：启动
第三阶段：运行
度量通道：
主控总线（EMMC/SPI/I2C master等）
度量通道：
低速通信总线（SPI/I2C slave等）
度量通道：
高速通信总线（USB/PCIE等）

图4　终端可信防护流程

2　系统实现

本文提出的TPCM可信终端架构方案与X86、ARM、MIPS等计算架构无关。主要支撑条件是主板具备主动度量端口、CPU通信端口及系统控制能力设计，如SPI、EMMC、I2C、USB、PCIE、GPIO等，所以并不局限于特定的计算平台和领域。以下实现以ARM CPU+RTOS（real time operating system）的网关终端为例进行原型实现。

可信网关终端系统组成如图5所示，可信防护系统主要由TPCM模块、可信代理和可信防护软件组成。当终端平台上电时，通过优先电源系统首先为TPCM提供电能，然后通过TPCM可信根确认启动代码的可信性。宿主系统在TPCM的控制下开机启动，通过启动可信代理程序采集系统执行环境信息并进行独立判定控制。最后通过操作系统代理支撑，动态度量和保持宿主系统的安全可信运行状态。

2.1　可信终端平台设计及可信控制实现

终端可信平台部件示意如图6所示，整个平台系统围绕着TPCM可信根为中心进行方案设计，图中斜杠表示受控部件或端口。在本文方案中，TPCM可信根被定义成终端系统运行和管控核心，SoC是计算部件，4G和以太网等是对外通信部件，电池等电源系统是电源部件，RS485、RS232x2、CAN、IO等为采集和内部通信端口，Real-Time Clock（RTC）、Watchdog Timer（WDT）等为辅助部件。当TPCM发现通信异常时，输出GPIO控制信号给控制执行部件实时阻断物理信道。TPCM通过主板端口控制系统配合，并根据预设信息进行用户设备使用权限部署，不同用户给予不同的设备访问权限。此外，对于重要的通信部件，TPCM根据策略进行流量监视和物理信道的控制。在判断机制系统的协助下，在TPCM确认通信或流量异常的情况下，将根据预先设定的策略进行信道干预。在极端情况下，切断其物理信道或关闭通信设备电源。

2.2　第一阶段系统待机度量实现

TPCM由独立电源供电，并通过电源控制信号对设备主电源进行控制。TPCM SPI控制器单元通过SPI总线与参数存储SPI闪存连接并仅向闪存供电。SPI控制器单元被配置为在TPCM上电后，从闪存中读取参数数据生成代码散列值的主控单元模块。散列值的生成可以按照现有技术进行，如SM3[24]。将散列值与参考散列值相比较。这里参数数据可根据用户防护策略选择为存储在闪存代码中的关键代码，如选择用于控制各硬件上电的代码，也可以选择其他关键数据、配置信息等。

同理，TPCM EMMC控制单元通过EMMC总线与闪存连接并根据策略实现对EMMC闪存中的数据进行度量保护。EMMC闪存中存有boot loader、操作系统代码、应用程序代码等。

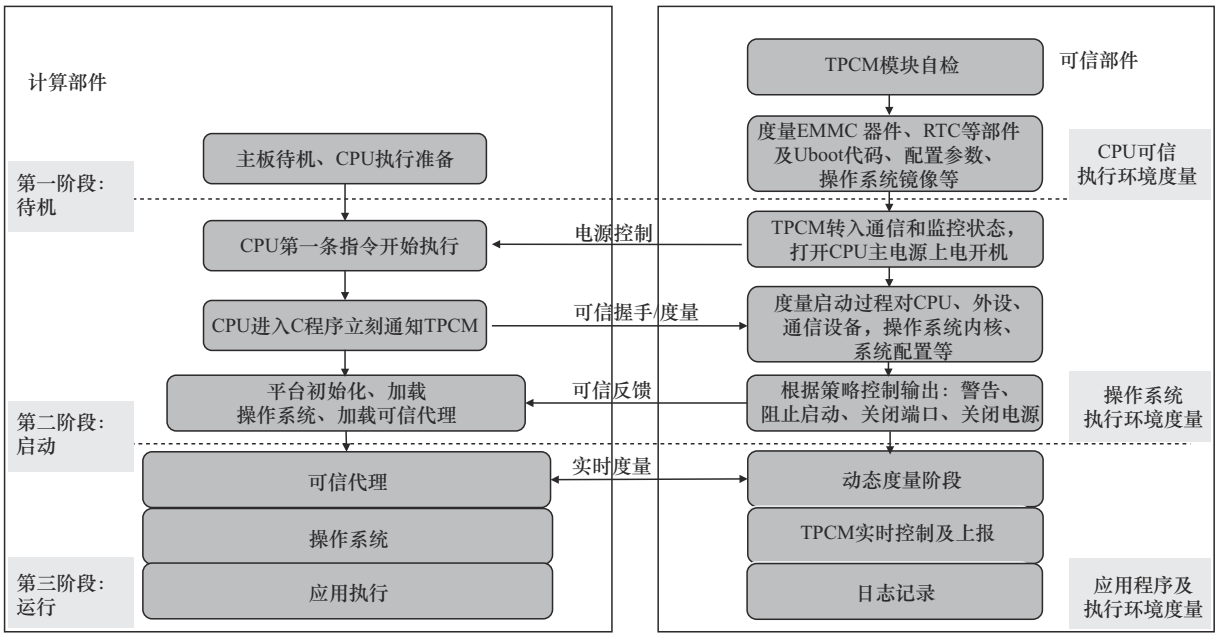


图5　可信网关终端系统组成

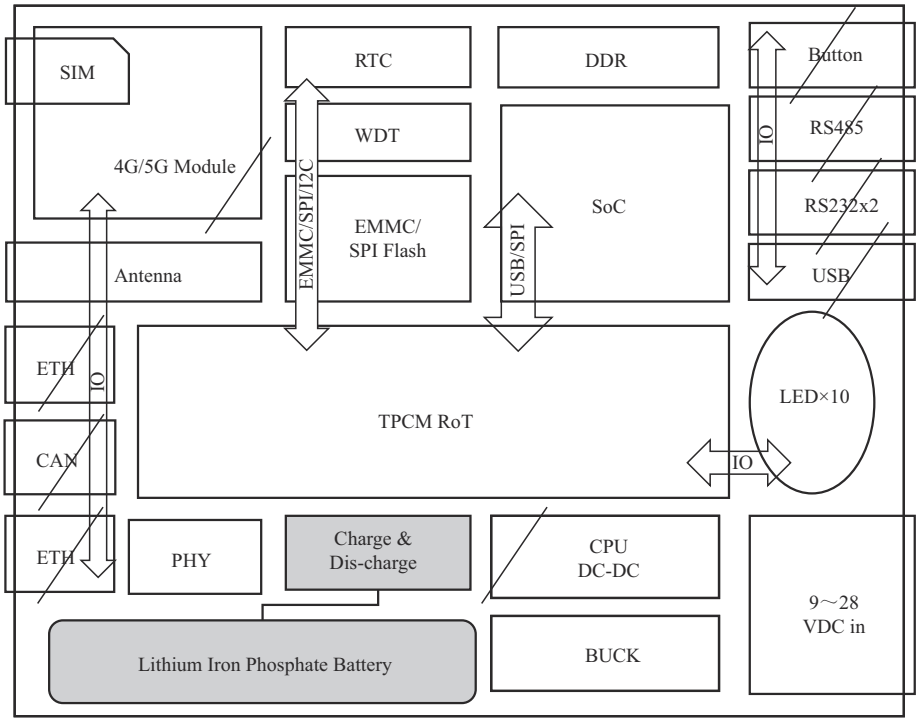


图6　终端可信平台部件示意

2.3　第二阶段启动过程度量实现

在第一阶段确保启动代码可信性和完整性的基础上，TPCM通过boot loader在启动代码中植入的可信代理，对启动环境进行检查确认[23]。若检测到可信环境遭受破坏或设备固件代码被恶意篡改，则根据预先写在TPCM内部的安全策略进入非可信工作模式或阻止计算机继续启动等。

TPCM度量信息通过SPI总线与计算单元连接交换数据信息。TPCM通过可信代理从计算机上获得设备的物理特征信息、代码信息等，如CPU、内存、网络设备、操作系统文件等。这里设备及代码数据可根据用户防护策略进行分级度量防护。

2.4　第三阶段动态度量实现及策略管理

图7说明了动态度量和策略下发机制。策略通过专门的安全管理通道进行管理下发，当TPCM通过身份识别、签名等手段确认策略指令的合法性后，通过TPCM私钥对策略指令进行解密分析，并将其存储于TPCM的可信策略管理单元。而策略下发只会发生在首次上电运行或策略更新时。

动态度量模块功能由TPCM动态度量引擎、过

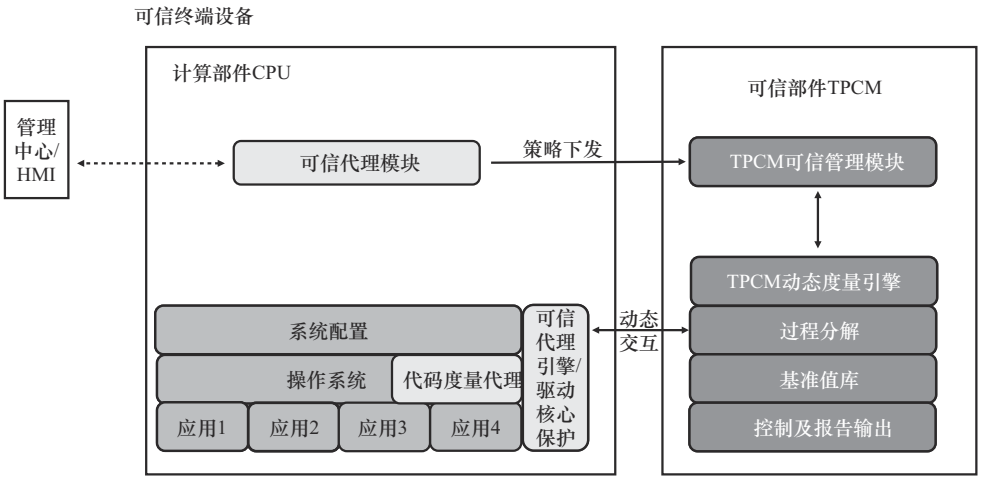


图7　动态度量和策略下发机制

程分解、基准值库、控制及报告输出组成，其中可信代理执行在计算CPU侧，协助TPCM截取程序代码信息及执行访问控制。可信代理运行在操作系统内核，功能包括TPCM驱动、可信协议和可信执行。可信代理是动态监测的重要组件，需TPCM在第一阶段EMMC代码主动度量和第二阶段操作系统加载到内存后进行2次代码可信度量确认，在第三阶段运行状态进行可信动态度量保障，保证可信代理的抗攻击性与不可绕过。

如图7所示，以操作系统加载应用1程序为例说明其过程。首先读取应用1程序文件并传递给TPCM，通过动态度量模块进行代码特征提取和完整性校验，确认应用程序的加载许可。在应用程序调入内存执行后，可信代理持续在TPCM的度量指令要求下通过可信OS度量执行机构获取应用程序在内存中的数据，并发送给TPCM进行可信判定。如果判定结果不可信则依据可信策略通过可信代理要求可信OS度量执行访问控制，同时依照策略通过TPCM自身控制机制进行物理控制保护或警告。

本文方案采用国产RTOS实现动态度量可信执行功能。根据TPCM度量指令要求的粒度不同，实现动态度量的执行对象可针对系统中的程序执行、某个关键行为或参数堆栈等分别进行度量，过程如下。

1) 根据可信代理发来的TPCM度量指令，请求对度量对象进行可信判断。

2) 如果是对程序进行度量，依照RTOS内核对内存的分区管理，如图8所示。因此，根据内核对内存的地址空间映射管理，可以找到操作系统以及应用程序模块相应的代码段起始位置和大小。

3) 如果需要对某一个关键行为进行度量，在操作系统中可将其具体映射为函数，在运行时系统中最终对应为一个符号，可以通过访问符号表来解析某个函数关键行为的信息，内核提供了symbol_lkup的接口原型来获取符号的内存地址和符号类型，该接口的原型定义为

```
int symbol_lkup (const char * name,
void ** value,
SymType * type
)
```

4) 如果需要进一步对某个任务的参数堆栈进行度量，则根据内核维护的任务控制块（TCB, task control block）实现，其定义如图9所示，可以获取任务的堆栈基址、栈大小等信息。

5) 平衡度量数据传输量的因素，将上述步骤获取的内容直接生成相应的散列值，并进行签名，

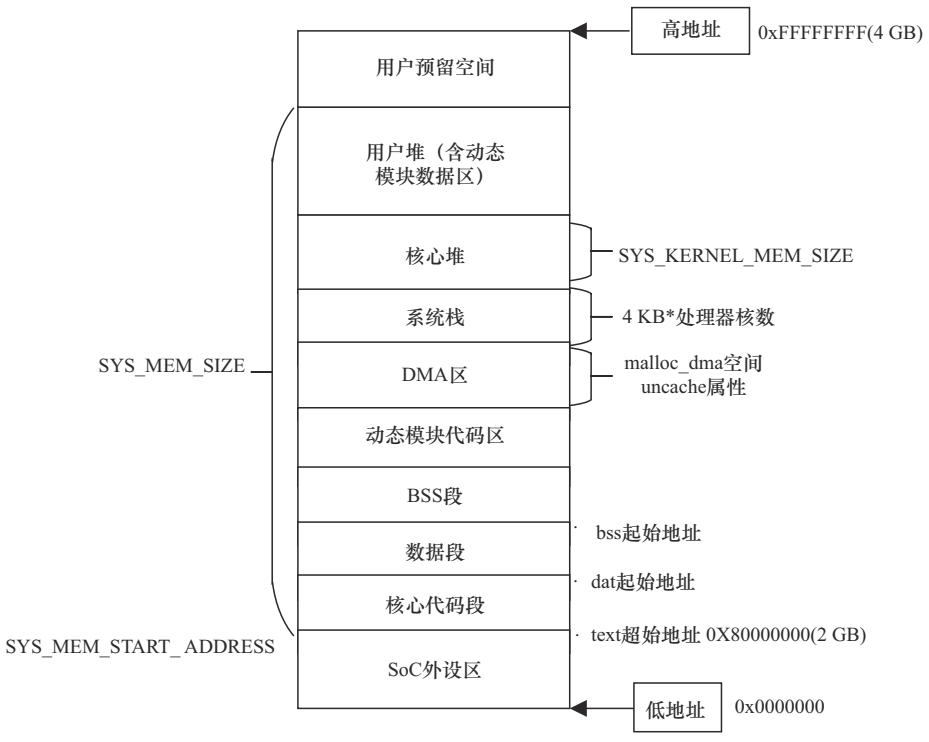


图8　代码段内存分区管理

作为提供给TPCM进行动态度量的内容。

6) 将散列值和签名值填入预先定义好的数据结构，交由可信代理引擎与TPCM进行交互，完成最终的动态度量。

```
typedef struct
{
    u32 td_id;
    task_type_t td_type;
    char *td_name;
    int td_priority;
    u32 td_status;
    u32 td_waitstatus;
    u32 td_real_pri ;
    int td_options;
    void(*td_entry)();
    u32 td_sp;
    u32 td_pc;
    void *td_pStackBase;
    u32 td_stackSize;
    int td_stackHigh;
    int td_stackMargin;
    int td_stackCurrent;
    int td_errorStatus;
    int td_timeout;
#ifdef __multi_core__
    cpuset_t td_affinity;
    int      td_running_cpu;
#endif
} Thread_Info;
```

图9　任务控制块定义

3　测试

3.1　测试环境

测试设备信息如表2所示。

表2　测试设备信息

设备	型号	数量
可信终端设备	迪石1010	1台
实时操作系统	锐华（ReWorks）可信RTOS	1套
调试笔记本	联想ThinkPad x1	1台
内存模拟攻击软件	VAT10	1套
USB设备	朗科（Netac）128 MB U盘	1个

3.2　测试结果

TPCM芯片模块嵌入设备主板，TPCM通过控制信号控制主电源对主板是否供电。主板上设计有iMX6ULL CPU计算系统、4G通信单元、以太网接口等。TPCM EMMC总线连接主板EMMC存储设备，进行boot loader及操作系统内核的读取。

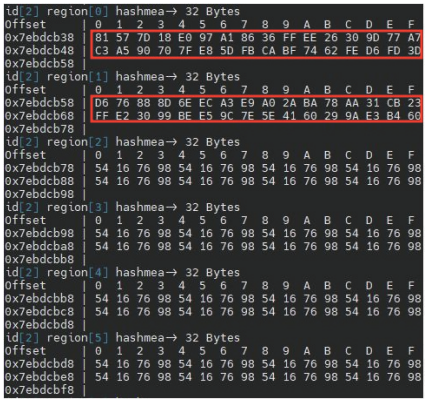
从接入电源开始监测记录过程。首先，录入可信基准信息。独立电源电路为TPCM芯片提供工作供电。当TPCM自检通过后，主动读取EMMC闪存代码并确认其可信性和完整性，如表3上半部分和图10所示度量值和可信状态。当可信度量状态检验通过后，控制终端设备主板上电。CPU上电boot loader执行过程中，通过boot loader中植入的可信代理获取CPU、操作系统核心文件配置等信息并记录到TPCM的基准值库中。其次，终端设备正常开机使用测试。重复上述开机过程，保持整机启动运行环境不变，正常开机进入操作系统，图11为可信终端设备启动日志。

表3下半部分和图12是通过终端设备修改固件后的度量结果和不可信状态。终端设备固件更新过程如图13所示。使用相同步骤进行模拟恶意替换设备部件或篡改部件固件实验。在终端设备启动前人为地替换成非法部件（如图14所示），或对操作系统加载代码进行篡改。TPCM在设备平台启动过程中立刻捕捉到周边部件及加载代码的变化，阻止设备平台启动并及时关闭设备系统电源。

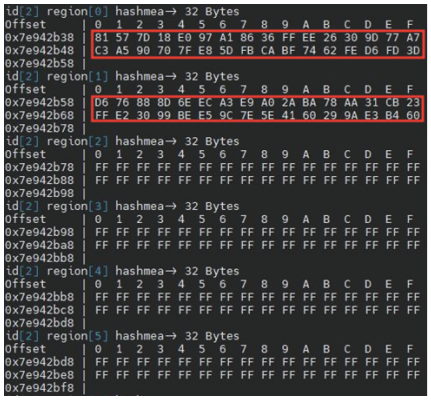
当终端设备运行在安全可信环境时，进行模拟攻击内存实验（如图15所示）。利用开发好的TPCM配置工具下发内存区域保护指令，并提供防护策略。TPCM接到指令后，激活动态度量模块防护，使之处于监控状态。此时，使用内存数值地址修改软件并修改该内存区域数据。该模块迅速发现异常并根据策略报告操作系统，同时，TPCM的可信软件基[25]根据防护策略判定风险级别并及时进行干预控制。

表3　模拟攻击EMMC闪存代码实验结果

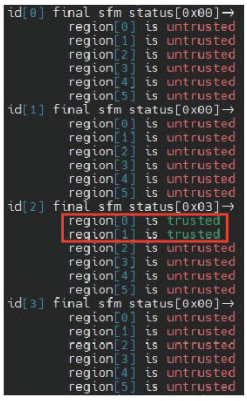
固件攻击测试	攻击位置	TPCM基准值	TPCM度量值	可信度量状态
攻击前	id[2]region[0]	81 57 7D 18 E0 97 A1 86 36 FF EE 26 30 9D 77 A7 C3 A5 90 70 7F E8 5D FB CA BF 74 62 FE D6 FD 3D	81 57 7D 18 E0 97 A1 86 36 FF EE 26 30 9D 77 A7 C3 A5 90 70 7F E8 5D FB CA BF 74 62 FE D6 FD 3D	通过
攻击前	id[2]region[1]	D6 76 88 8D 6E EC A3 E9 A0 2A BA 78 AA 31 CB 23 FF E2 30 99 BE E5 9C 7E 5E 41 60 29 9A E3 B4 60	D6 76 88 8D 6E EC A3 E9 A0 2A BA 78 AA 31 CB 23 FF E2 30 99 BE E5 9C 7E 5E 41 60 29 9A E3 B4 60	通过
攻击后	id[2]region[0]	A3 5A 10 4A 3A 1E 99 1D 3D 14 89 10 C1 85 D3 B0 39 C1 CA 89 7F 68 C4 34 54 39 E6 4C EB 47 43 85	81 57 7D 18 E0 97 A1 86 36 FF EE 26 30 9D 77 A7 C3 A5 90 70 7F E8 5D FB CA BF 74 62 FE D6 FD 3D	不通过
攻击后	id[2]region[1]	D6 76 88 8D 6E EC A3 E9 A0 2A BA 78 AA 31 CB 23 FF E2 30 99 BE E5 9C 7E 5E 41 60 29 9A E3 B4 60	7B 38 45 E0 C3 FC 63 1E C6 7A E0 DA DF 5B 08 42 A6 50 30 B0 0A 6A E4 C2 04 26 FE C8 8B A2 51 A0	不通过



(a) EMMC闪存id[2] region[0/1]区域基准值



(b) EMMC闪存id[2] region[0/1]区域度量值



(c) EMMC闪存id[2] region[0/1]区域可信状态

图10　EMMC闪存代码篡改前TPCM度量结果

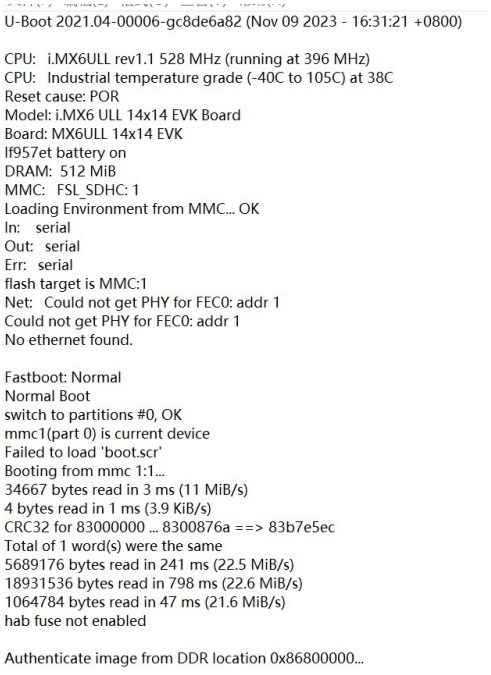


图11　可信终端设备启动日志

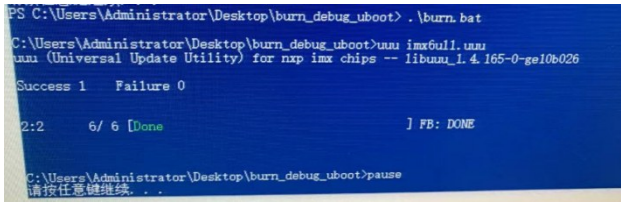
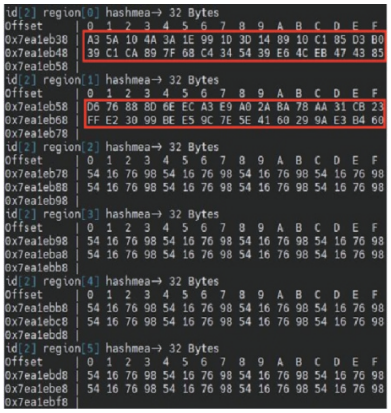


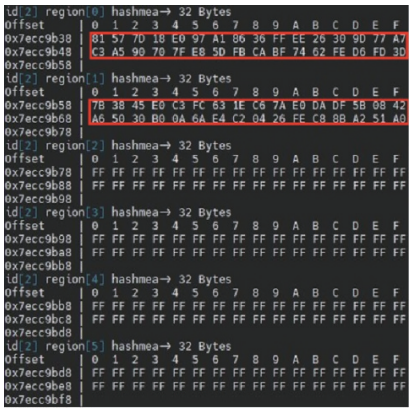
图13　终端设备固件更新过程

此外，还对终端设备部件或外设进行实时替换或添减实验。当部件或外设发生改变时，动态防御模块能快速感知系统平台的变化，并根据策略做出对应的控制。当一个未知USB外设接入终端设备时，TPCM则迅速关闭该外设USB端口，禁止其连接系统（如图16所示）。

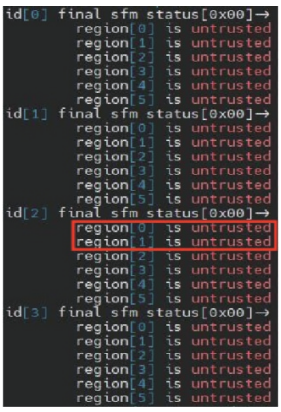
以上测试在多种应用场景下经过多天的压力测试，均达到了防护目的。当运行环境正常可信时，丝毫不影响原系统的启动运行机理和可信状态，终端设备系统工作正常稳定。



(a) EMMC闪存id[2] region[0/1]区域基准值



(b) EMMC闪存id[2] region[0/1]区域度量值



(c) EMMC闪存id[2] region[0/1]区域不可信状态

图12　EMMC闪存代码篡改后TPCM度量结果

```
Bus 002 Device 002: ID 1677:0102
Bus 001 Device 001: ID 1d6b:0002
Bus 001 Device 004: ID 2c7c:0901
Bus 001 Device 002: ID 0424:2514
Bus 002 Device 001: ID 1d6b:0002
Bus 001 Device 005: ID 0dd8:f607
tpcmss_executephase2: failed, rc 0x00000101
TPCM_RC_FAILURE - commands not being accepted because of a TPCM failure
tpcmapi_executephase2:executephase2 fail[0x00000101]
tpcmapi_executephase2 fail - 0x00000101
```

图 14　设备替换模拟攻击及 TPCM 度量结果

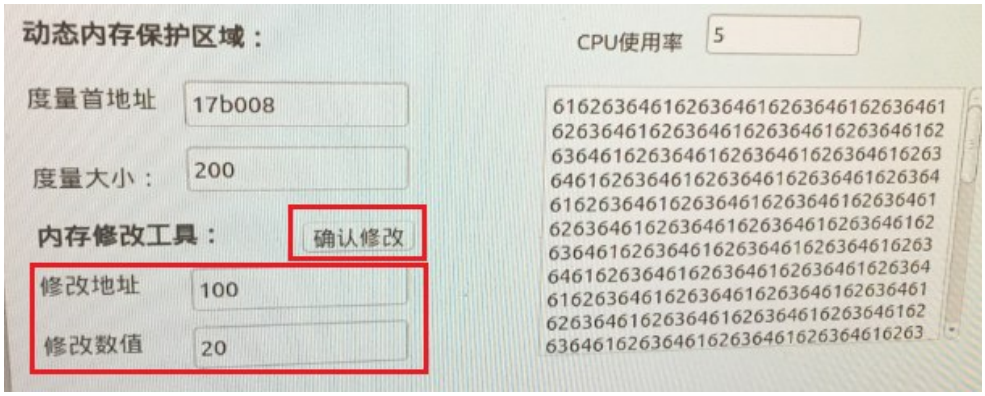
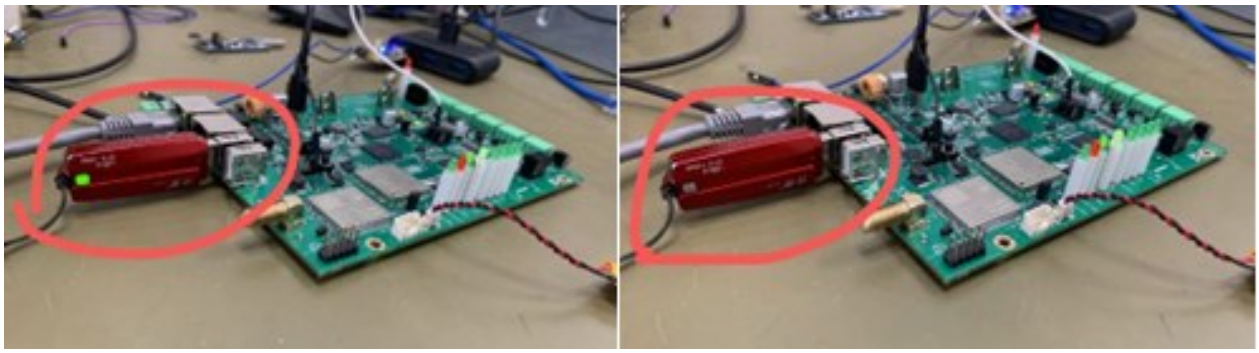


图 15　TPCM 动态内存防护测试及模拟攻击



```
root@lf957ss:/mnt/app/tpcm/test2# ./read_std_mea_sts 2 std
device0  3FFBF0CDB15FA8253858645D828305E4DE3DA183F365AF84A8824A5F79CD523E
root@lf957ss:/mnt/app/tpcm/test2#
```

```
root@lf957ss:/mnt/app/tpcm/test2# ./read_std_mea_sts 2 mea
device0  EB52D739C54FB19828A513343A0D2CDC28E42B60C04FB992546D7B14C159F84A
root@lf957ss:/mnt/app/tpcm/test2#
```

```
root@lf957ss:/mnt/app/tpcm/test2# ./read_std_mea_sts 2 sts
device0 untrusted
root@lf957ss:/mnt/app/tpcm/test2#
```

图 16　模拟非法 USB 设备攻击及 TPCM 度量防护

4　结束语

针对 BP 机爆炸类似事件，假设终端设备引入基于 TPCM 可信根的双体系可信架构设计（为避免合谋攻击的可能性，TPCM 可信根芯片由最终用户或指定可信赖供应商提供），类似终端设备的病毒入侵和远程非法操控难度会大幅度增加，事件发生概率也就会相应降低。可信终端设计时应重点考虑以下事项。1) 设备需要在硬件设计时植入完全独

立可控的硬件TPCM可信根芯片。2) 基于双体系结构进行软硬件设计，确保防护系统度量、分析和控制的独立性。3) 具备设备全生命周期的主动度量、动态防护（控制）能力。

本文结合计算机体系结构和TPCM可信根技术，提出了基于双体系思想的可信终端架构。通过主动度量、可信扩展、可信判定和可信控制，构造具有独立可信度量和防护能力的终端平台架构。该架构采用国家标准定义的可信平台控制模块作为信任硬件根源对终端设备系统整个运行过程进行保护，实现可信终端设备全过程安全可信。在未来工作中，一方面，研究将本文提出的可信终端架构用于双体系结构的可信网络管理系统，通过基础设施及网络节点平台的静态和动态度量技术，解决网络节点执行环境认证、平台身份认证、平台执行代码及端口可信管理等问题，构建独立可信管理中心，实现节点可信策略下发、动态度量管理、智能分析及态势感知能力等网络安全可信能力。另一方面，针对具体应用场景的安全等级要求、设备功耗、成本等考量因素对架构进行优化和配置，提高可信终端设备整体效率及适应范围。

参考文献：

[1] 沈昌祥, 田楠. 主动免疫可信计算打造安全可信网络产业生态体系[J]. 信息通信技术与政策, 2022(8): 1-6.
SHEN C X, TIAN N. Active immune trusted computing to create a secure and trusted network industry ecosystem[J]. Information and Communications Technology and Policy, 2022(8): 1-6.

[2] 张建标, 黄浩翔, 胡俊. 主动免疫可信计算综述[J]. 中兴通讯技术, 2022, 28(6): 12-16.
ZHANG J B, HUANG H X, HU J. A survey on active immune trusted computing[J]. ZTE Technology Journal, 2022, 28(6): 12-16.

[3] Trusted Computing Group. TPM main specification[R]. 2009.

[4] Trusted Computing Group. PC client platform TPM profile (PTP) specification[R]. 2023.

[5] 尚文利, 张修乐, 刘贤达, 等. 工控网络局域可信计算环境构建方法与验证[J]. 信息网络安全, 2019, 19(4): 1-10.
SHANG W L, ZHANG X L, LIU X D, et al. Construction method and verification of local trusted computing environment in industrial control network[J]. Netinfo Security, 2019, 19(4): 1-10.

[6] CHALLENER D, YODER K, CATHERMAN R, et al. A practical guide to trusted computing[M]. Beijing: Machinery Industry Press. 2009.

[7] 杨维永, 刘苇, 崔恒志, 等. SG-Edge: 电力物联网可信边缘计算框架关键技术[J]. 软件学报, 2022, 33(2): 641-663.
YANG W Y, LIU W, CUI H Z, et al. SG-Edge: key technology of power Internet of things trusted edge computing framework[J]. Journal of Software, 2022, 33(2): 641-663.

[8] 崔津华, 蔡志平, 刘柯江. SGX隔离技术研究综述[J]. 华中科技大学学报(自然科学版), 2024, 52(2): 1-15.
CUI J H, CAI Z P, LIU K J. A survey on SGX isolation technology[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2024, 52(2): 1-15.

[9] 刘永志, 秦桂云, 刘蓬涛, 等. 可证明安全的基于SGX的公钥认证可搜索加密方案[J]. 计算机研究与发展, 2023, 60(12): 2709-2724.
LIU Y Z, QIN G Y, LIU P T, et al. Provably secure public key authenticated encryption with keyword search based on SGX[J]. Journal of Computer Research and Development, 2023, 60(12): 2709-2724.

[10] GlobalPlatform. Introduction to trusted execution environments[R]. 2018.

[11] NGABONZIZA B, MARTIN D, BAILEY A, et al. TrustZone explained: architectural features and use cases[C]//Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). Piscataway: IEEE Press, 2016: 445-451.

[12] 李志鹏. 基于TrustZone的强制访问控制安全增强机制研究[D]. 长沙: 国防科技大学, 2022.
LI Z P. Research on security enhancement mechanism of mandatory access control based on TrustZone[D]. Changsha: National University of Defense Technology, 2022.

[13] 王奕钧. 基于零信任机制的工业互联网边界防护方案研究[J]. 计算机技术与发展, 2024, 34(3): 96-101.
WANG Y J. Research on border protection scheme of industrial Internet based on zero trust mechanism[J]. Computer Technology and Development, 2024, 34(3): 96-101.

[14] 郭颖, 毛军捷, 张翀斌, 等. 基于可信平台控制模块的主动度量方法[J]. 清华大学学报(自然科学版), 2012, 52(10): 1465-1473.
GUO Y, MAO J J, ZHANG C B, et al. Active measures based on a trusted platform control module[J]. Journal of Tsinghua University (Science and Technology), 2012, 52(10): 1465-1473.

[15] 国家标准化管理委员会. 信息安全技术 可信计算规范 可信平台控制模块: GB/T 40650-2021[S]. 北京: 中国标准出版社, 2021.
Standardization Administration of the People's Republic of China. Information security technology-trusted computing specification-trusted platform control module: GB/T 40650-2021[S]. Beijing: Standards Press of China, 2021.

[16] 沈昌祥. 网络强国系列 用可信计算3.0筑牢网络安全防线[J]. 信息安全研究, 2017, 3(4): 290-298.
SHEN C X. Building cyber security defense by trusted computing 3.0[J]. Journal of Information Security Research, 2017, 3(4): 290-298.

[17] 沈昌祥. 创新发展主动免疫可信计算筑牢网络强国、数字中国安全可信底座[J]. 网络空间安全科学学报, 2023(1): 1-16.
SHEN C X. Innovation-driven development of active immunity trusted computing, building a secure and trustworthy foundation for cyber power and digital China[J]. Journal of Cybersecurity, 2023(1): 1-16.

[18] 黄坚会, 沈昌祥, 谢文录. TPCM三阶三路安全可信平台防护架构[J]. 武汉大学学报(理学版), 2018, 64(2): 109-114.

HUANG J H, SHEN C X, XIE W L. The TPCM 3P3C defense architecture of safety and trusted platform[J]. Journal of Wuhan University (Natural Science Edition), 2018, 64(2): 109-114.

[19] 黄坚会, 沈昌祥. TPCM主动防御可信服务器平台设计[J]. 郑州大学学报(理学版), 2019, 51(3): 1-6.
HUANG J H, SHEN C X. Trusted platform design of server with TPCM active defense[J]. Journal of Zhengzhou University (Natural Science Edition), 2019, 51(3): 1-6.

[20] HUANG J H, SHEN C X, ZHANG J B, et al. A trusted execution environment architecture for big data computing platform based on TPCM[C]// Proceedings of the 2023 13th International Conference on Communication and Network Security. New York: ACM Press, 2024: 88-93.

[21] 国家密码管理局. GB/T29829. 可信计算密码支撑平台功能与接口规范[S]. 北京: 标准出版社, 2013.
National Cryptography Administration. GB/T29829. Trusted computing password support platform function and interface specification[S]. Beijing: Standard Press, 2013.

[22] 黄坚会. TPCM可信平台度量及控制设计[J]. 信息安全研究, 2017, 3(4): 310-315.
HUANG J H. The TPCM platform measurement and control design[J]. Information Security Research, 2017, 3(4): 310-315.

[23] 黄坚会. 中国可信平台控制模块[M]. 北京:中国大百科全书, 2022.
HUANG J H. China trusted platform control module[M]. Beijing: Encyclopedia of China, 2022.

[24] 国家密码管理局. SM3密码杂凑算法: GM/T 0004-2012[S]. 北京: 中国标准出版社, 2012.
National Cryptography Administration. SM3 cryptographic hash algorithm: GM/T 0004-2012[S]. Beijing: Standards Press of China, 2012.

[25] SHI W C. On design of a trusted software base with support of TPCM[C]// Trusted Systems. Berlin: Springer, 2010: 1-15.

[作者简介]

黄坚会（1979– ），男，广东江门人，北京工业大学博士生，主要研究方向为系统安全、网络空间安全和可信计算。

张江江（1994– ），男，山西临汾人，山西大学讲师，主要研究方向为大数据建模及优化、隐私保护、网络空间安全和可信计算。

沈昌祥（1940– ），男，浙江宁波人，中国工程院院士，北京工业大学教授、博士生导师，主要研究方向为可信计算、密码学安全等。

张建标（1969– ），男，江苏海门人，北京工业大学教授、博士生导师，主要研究方向为可信计算、系统安全。