可信技术在国产化嵌入式平台的应用研究

孟祥斌，刘笑凯，郝克林
（华北计算机系统工程研究所，北京 100083）

摘　要： 国产化嵌入式平台的安全威胁依旧严峻，为了提高国产化平台的安全性与可控性，可信技术的应用十分关键。在基于龙芯 2K-1000CPU 的国产化嵌入式平台上，采用可信平台控制模块（Trusted Platform Control Module，TPCM），应用可信启动、可信软件基、可信文件存储和 I/O 口的可信访问等技术，实现了国产化嵌入式平台的可信运行。TPCM 可信模块基于 CCP903T 密码芯片实现。此平台已在某安全项目中通过测试投入使用，对可信技术在国产化平台的应用以及标准化形成留下参考性意义。

关键词： 可信启动；可信平台控制模块；国产化平台；I/O 口可信访问
中图分类号： TN918；TP309　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.211350

中文引用格式： 孟祥斌，刘笑凯，郝克林. 可信技术在国产化嵌入式平台的应用研究[J]. 电子技术应用，2021，47(12)：94-99.
英文引用格式： Meng Xiangbin，Liu Xiaokai，Hao Kelin. Research on application of trusted technology in localized embedded platform[J]. Application of Electronic Technique，2021，47(12)：94-99.

Research on application of trusted technology in localized embedded platform

Meng Xiangbin，Liu Xiaokai，Hao Kelin
（National Computer System Engineering Research Institute of China，Beijing 100083，China）

Abstract： The security threats of localized embedded platforms are still severe. In order to improve the security and controllability of localized platforms, the application of trusted technology is critical. This article uses a trusted platform control module(TPCM) on a localized embedded platform based on the Godson 2K-1000CPU, using trusted boot, trusted software base, trusted file storage and I/O ports. Technology such as trusted access realizes the trusted operation of the localized embedded platform. The TPCM trusted module is implemented based on the CCP903T cryptographic chip. This platform has been tested and put into use in a security project, leaving a reference for the application of trusted technology in the localization platform and the formation of standardization.

Key words： trusted boot；trusted platform control module(TPCM)；localization platform；I/O port trusted access

0 引言

近些年计算机技术飞速发展，同时信息安全威胁事件大量爆发，信息安全问题被国内外各研究人员广泛关注。传统的信息安全防御技术有防火墙、堵漏洞以及入侵检测等方式，很难有较大突破。沈昌祥院士提出：网络安全最重要的是“安全可信”[1]。我国在“自主研发”方面实现了信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控，但是由于计算机体系结构固有的缺点以及软件可能存在的缺陷，在自主研发的平台下，仍然存在各种不可避免的未知的软硬件漏洞。因此，本文将运用可信技术，遵照可信计算规范，自主设计可信硬件模块，扩展可信 BIOS 和操作系统。以可信密码模块为信任根，构建贯穿硬件层、固件层、操作系统层和应用层全过程的信任链解决方案，能够为国产化嵌入式计算平台提供有效完整的全信任链保护，实现了信息系统基础平台装备的“安全可信”。

1 可信计算概述

可信计算从 1983 年开始在国内外一直备受学者们关注，可信计算经历了三个时代：(1)可信 1.0 时代：容错计算，其主要采取容错算法和冗余备份等技术提高大型机时代主机的可靠性[2]；(2)可信 2.0 时代：被动可信体系，可信 2.0 的理念是从硬件层面的可信根出发，建立从可信根到操作系统再到应用层面的可信链，以此完成可信度量和可信存储等功能；(3)可信 3.0 时代：主动免疫体系[3]，可信节点的建立和与系统的交互是可信 3.0 的关键，可信 3.0 的主动监控机制不需要修改现有系统环境即可提供可信支撑，其还可将可信计算的定义权交给属主自己，为属主提供极高的自由度，主动可信机制将可信计算功能封装在可信子系统中，简单化和规范化的可信子系统为开发工作提供便利，可信 3.0 主动免疫

体系在我国发展迅速，在很多领域的实际应用效果显著[4]。本文将主动免疫体系的可信计算技术应用到全国产化嵌入式平台。

2 可信技术在国产化平台的应用

2.1 国产化嵌入式硬件平台设计

(1)硬件平台设计

自主安全国产化平台组成框图如图 1 所示，主要由龙芯 2K-1000 处理器模块[5]、存储 CRTM 的 Nor Flash 存储器、CPLD 控制器、NAND Flash 存储器、4 个千兆网口、1 个串口、高云 GW2A-55FPGA 以及基于 CCP903T 芯片的 TPCM 可信模块组成。其中，可信硬件模块通过 miniPCIE 插卡形式接入板卡，嵌入式平台通过串口和网口进行调试。

(2)基于 CCP903T 的可信模块简介

此平台可信模块是基于 CCP903T 单核芯片设计的一款具有高速密码服务的密码模块，遵循国家密码管理局关于 PCI 密码模块的相关规范，支持 SM1、SM2、SM3、SM4 等国密算法；支持 PCIE x4 lanes，能够为各类可信安全平台提供多线程、多进程和多卡并行处理的高速密码运算服务，其可以提供数字签名/验证、非对称/对称加解密、数据完整性校验、真随机数生成、密钥生成及管理等功能，可以保证敏感数据的机密性、真实性、完成性和抗抵赖性，此可信模块满足国产化自主安全、性能高、成本低等原则[6]。

2.2 国产化可信嵌入式平台软件设计

基于龙芯 2K-1000 CPU 的国产化嵌入式可信平台的软件设计如图 2 所示。

2.2.1 可信启动

嵌入式系统上电后，首先会执行 BIOS 程序，进行硬件初始化，建立内存映射图，将系统配置到理想状态；然后再读取内核映像文件，并写入内存；最后跳入内核入口进行嵌入式操作系统的启动[7]。嵌入式系统存储器具有固态非易失性，如 EEROM 和 Flash 等，大多数情况下内核映像和根文件系统应用其存储[8]。

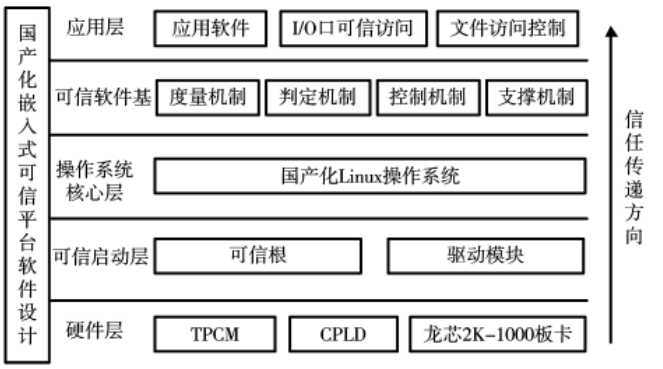

图 2 软件设计架构

此国产化嵌入式平台经过改造后加入一个存储 CRTM 和标准摘要值的 Nor Flash、CPLD 控制器以及 TPCM 可信模块，通过 CPLD 控制器控制整个可信启动过程的各个阶段，也就是 Nor Flash、CPLD、TPCM 以及 CPU 分别在不同时刻取得控制权，四者在不同时刻分别作为运算的核心部件。系统上电后 CPLD 控制器首先取得控制权，使 CPU 与外设之间的连接都断开，阻止 CPU 启动，先启动 TPCM 模块和 Nor Flash，运行 CRTM 可信根，CRTM 读取内存中预存的 TPCM 命令库并调用 TPCM 中的 SM-3 算法引擎，将命令库发给 TPCM，TPCM 对收到的数据进行度量并将结果扩展到 PCR0。CRTM 读取 PCR0 中的摘要值，并与片内预存的标准摘要值进行对比，如果对比结果相同则继续启动，否则停止。然后 CRTM 会以同样的方式对标准值扩展库、BIOS 程序、Bootloader 引导加载程序进行度量，若 Bootloader 可信则 CPLD 控制器复位 CPU，运行 Bootloader，CPU 获取控制权。

随后 Bootloader 依次调用 TPCM 对内核映像和根文

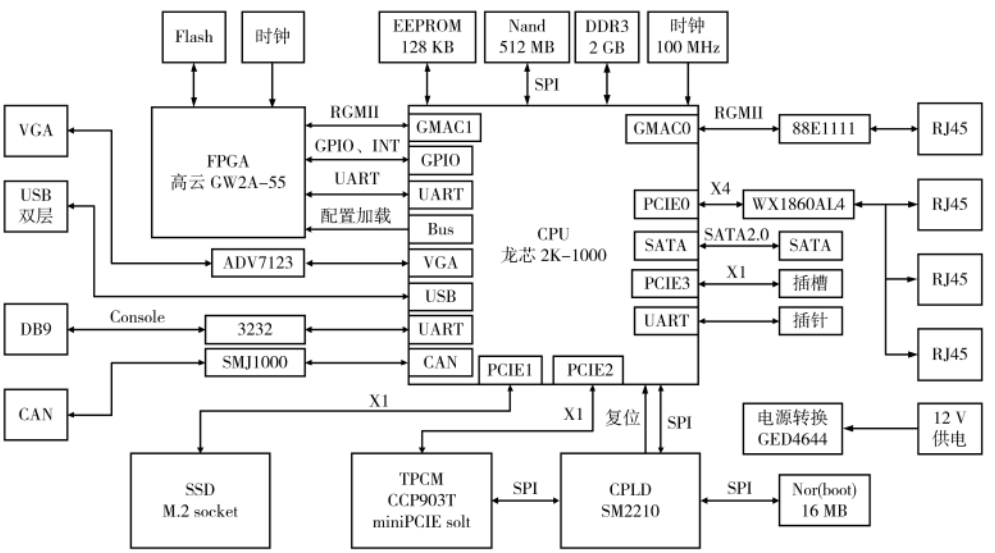

图 1 自主安全的国产化硬件平台组成框图

件系统进行度量，若结果都可信，说明内核代码没有被篡改过，则可以启动嵌入式系统内核。具体可信启动流程如图 3 所示。

2.2.2 可信软件基

国产化嵌入式平台可信启动成功，操作系统开始运行，随后会有大量程序运行和应用软件启动，系统运行

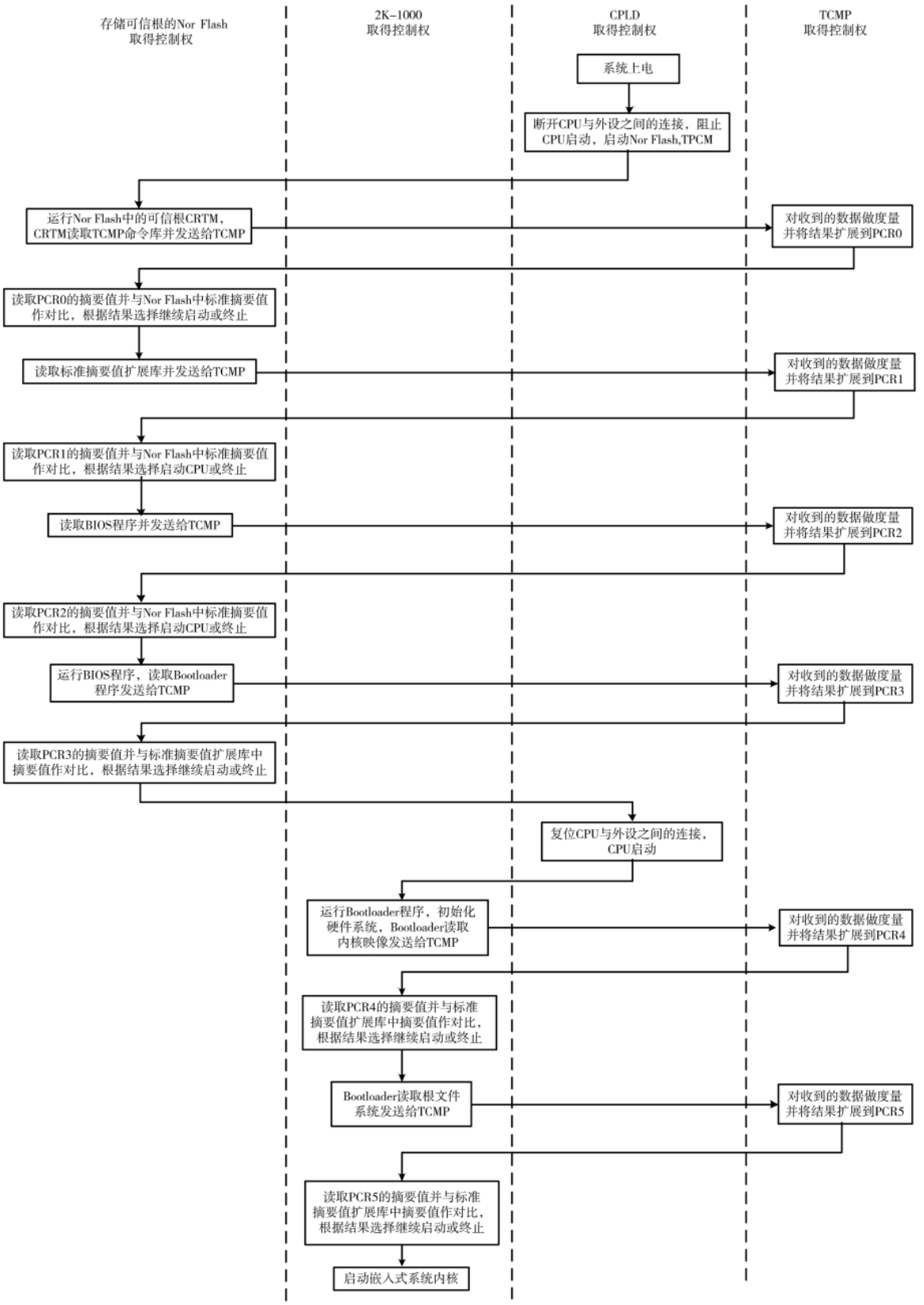

图 3　可信启动流程

任务繁重，运行环境复杂，此后更加容易受到持续的安全威胁。由于 TPCM 安全芯片主要提供安全核心的密码学功能，其存储和计算能力薄弱，需要可信软件基 TSB 代理 TPCM 的可信管理功能，支撑系统的可信运行环境。可信软件基的组成机制如图 4 所示。

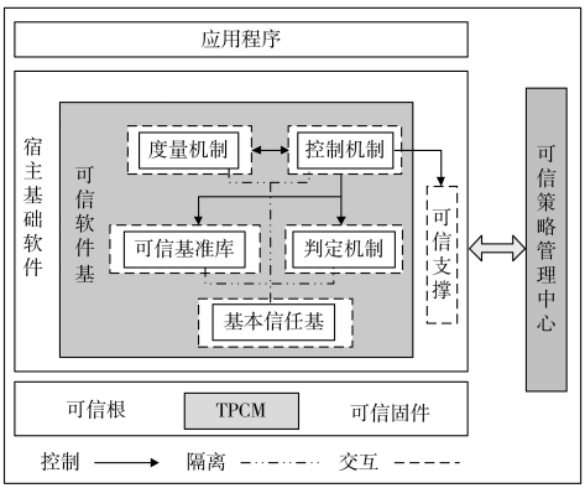

图 4 可信软件基 TSB 组成机制

可信软件基在整个国产化嵌入式可信平台中承担着承上启下的作用，对上保护操作系统中运行的应用程序，对下调用 TPCM 安全芯片的功能接口并管理 TPCM 中其他可信资源[9]。

可信软件基由宿主系统中多个可信功能软件互联互通构成，并不是一个独立系统，TSB 包括度量机制、控制机制、判定机制、可信基准库和基本信任基等主要部件[10]。其基本信任基由 TPCM 的可信根提供，为可信软件基提供基本可信功能；可信基准库为可信度量、控制、管理和判定提供基准可信资源；TSB 的度量机制计算可信计算平台系统应用软件的度量值；根据度量机制产生的度量值和系统规则判定机制推导其是否可信；根据度量值、判定结论和可信基准库中的基准控制策略，控制机制向 TPCM 安全芯片发送控制指令；支撑机制为应用系统提供可信密码服务和其他可信服务，支持可信软件基对安全芯片 TPCM 的访问与控制，并将可信资源传给 TSB 内部和可信基准库，供 TSB 使用。

国产化嵌入式操作系统可信启动后，则运行实现业务的应用软件，应用软件执行需要配置文件和动态库文件支撑。在运行应用软件前可信软件基的度量机制调用 TPCM 安全芯片的 SM-3 算法引擎对应用程序进行度量，将度量结果扩展到 PCR 寄存器，可信软件基的判断机制读取 PCR 寄存器中的度量值并与可信基准库中标准摘要值进行对比，根据判定结果可知应用程序是否被篡改，从而控制机制决定应用软件是否运行。运行过程中需要加载系统文件时，根据同样的度量、判定和控制机制进行文件的可信度量，控制其是否可被加载。

应用程序的可信执行建立在系统已可信启动进入可信运行环境的基础上，应用程序执行过程中的可信度量由可信软件基的控制机制、度量机制、判定机制以及可信基准库配合 TPCM 可信硬件模块共同完成。

2.2.3 可信平台下文件存储与操作

传统国产化嵌入式平台的加密文件系统是将密钥加密存储在磁盘，这种方式大大降低密钥管理的安全性，整个系统缺少可信计算基，给加解密模块带来严重安全威胁[11]。目前国产化可信嵌入式平台的文件加解密系统仍存在一定问题，如密钥存储的安全性、不能对文件粒度进行加密保护导致加解密粒度过粗等问题。

下面针对目前存在的问题设计此嵌入式平台的密钥管理模块、文件加解密服务和文件完整性校验模块。

(1)密钥管理模块

密钥的安全管理是影响整个可信平台可靠性的重要因素，此平台的密钥管理采用分层加密思想，可信根中的存储根密钥(SRK)作为源头，建立可信链，将可信传递给密钥和文件。可信存储根密钥永远存放在可信根内部，当使用 SRK 时，必须将需要加密的文件传到可信根内部，加密完成后再将密文对外传递使用。当文件需要机密性保护时，系统调用 TPCM 的随机数生成器生成存储密钥，系统中对每个用户 TPCM 会生成一个用户加密密钥，用户加密密钥将存储密钥加密，再将加密后的数据传给可信根，用 SRK 进行加密，再将最终密文存储到底层文件系统。此密钥管理方式是用 SRK 保护用户加密密钥，使用用户加密密钥保护存储密钥。此分层密钥管理模式提高了密钥存储的可靠性与安全性。密钥管理流程如图 5 所示。

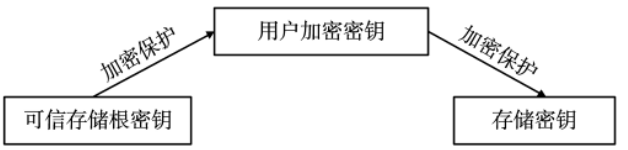

图 5 密钥管理流程图

(2)文件加解密模块

此国产化嵌入式平台的文件加解密服务采用 SM4 对称加密算法。文件需要机密性保护时，用户调用 TPCM 中 SM4 算法引擎，并与密钥管理模块交互获得存储密钥，文件加解密模块将加密后的文件密文存储在底层文件系统。加解密模块最重要的就是保护存储密钥的安全性，本文采用分层密钥管理的方式保证密钥安全性。

(3)文件完整性校验模块

完整性校验采用 HMAC 机制实现，HMAC 是散列函数消息码鉴别机制。此平台 HMAC 机制通过采用 TPCM 中 SM3 杂凑算法和存储密钥来实现。

2.2.4 I/O 口可信认证

I/O 口的可信访问主要基于身份认证机制和访问控制机制[12]，用户只有通过身份认证机制后，才能通过访

问控制机制进行 I/O 口的使用。此平台的 I/O 口主要包括网卡、显示屏、LED 灯、开关机键、身份认证口、主备按键、串口以及销毁键等。I/O 口的可信访问流程如图 6 所示。

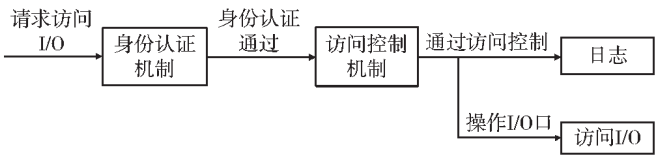

图 6 I/O 口可信访问流程

(1)身份认证机制

传统的身份认证一般是通过“用户名+密码”的方式[13]，一旦密码丢失，系统中重要信息就会被攻击者窃取或篡改，此国产化平台采用 USB 身份钥匙配合 TPCM 模块进行身份认证，USB 身份钥匙中包含用户 ID、用户访问权限以及用于身份认证的私钥，身份认证私钥存储在 TPCM 模块内存中，具体身份认证流程如下：

①USB 身份钥匙插入此平台，TSB 调用 TPCM 中 SM2 算法引擎对 USB 中存储的身份信息进行可信度量，若度量值与基准值不匹配则停止访问；

②确认身份信息没有被篡改，TPCM 的随机数生成器生成一串随机数；

③TPCM 用 SM4 算法将随机数进行加密，生成密文 C；

④TPCM 分别从 USB 和内存中读取身份认证私钥合并成完成私钥；

⑤用身份认证私钥对密文 C 解密，若解密成功则身份认证成功；

⑥访问控制机制读取 USB 中的用户访问权限信息并存储。

(2)访问控制机制

访问控制机制主要限制非法使用户和越权访问用户[14]，访问控制一般有 3 种类型，基于身份的访问控制(DAC)、基于规则的访问控制(MAC)和基于角色的访问控制(RBAC)。DAC 灵活性高，但控制能力差；MAC 控制能力强，但灵活性低[15]；综合考虑本平台采用基于角色的访问控制。此平台用户分为非法用户、普通用户和管理员用户，非法用户禁止访问 I/O 口，普通用户也称为受限用户，其只能访问一部分 I/O 口，此平台用户分类以及访问权限划分如表 1 所示。

表 1 用户访问权限表

	非法用户	普通用户	管理员用户
显示屏	拒绝	读写	读写
LED 灯	拒绝	读写	读写
开关机键	拒绝	读写	读写
串口	拒绝	读写	读写
身份认证 USB 口	只读	只读	读写
网卡	拒绝	读写	读写
销毁键	拒绝	拒绝	读写

(3)销毁键可信访问具体实现

销毁键在此平台 I/O 口中属于高安全级别按键，不能随意将密码资源销毁。因此需要访问控制机制进行管控。具体流程如下：

①销毁键按下，销毁线程检测到销毁键按下操作；

②钩子函数截获程序的执行，进行用户身份的确认；

③若为管理员用户则放行此操作，否则禁止访问。

3 演示验证

此国产化可信嵌入式平台已在某卫星项目中投入使用，使用状况良好，基于此平台进行可信技术的测试验证。

可信度量测试中，未篡改可执行程序可以正常运行，篡改过的可执行程序 error。未篡改的应用程序请求执行如图 7 所示，应用程序篡改后请求执行如图 8 所示。

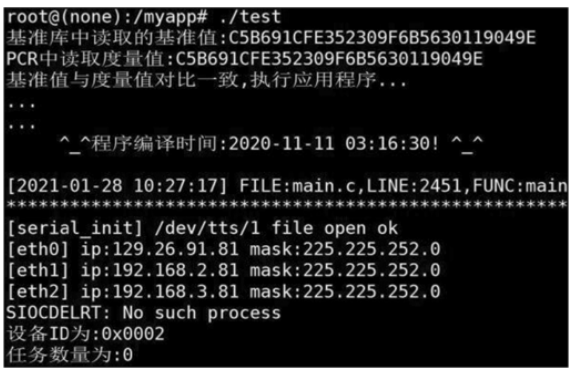

图 7 应用程序执行成功

图 8 应用程序执行失败

4 结论

本文实现了基于龙芯 2K-1000 CPU 的国产化嵌入式平台的“安全可信”。应用可信启动、可信软件基、可信存储和可信 I/O 访问等可信技术实现国产化嵌入式平台的可信运行，此可信的国产化嵌入式平台已在某卫星项目投入使用，这对以后国产化嵌入式平台可信技术的应用以及标准化形成有参考性意义。

参考文献

[1] 沈昌祥，彭科峰.用可信计算构筑网络安全防护体系[N].

中国科学报,2016-05-17(001).
[2] 胡俊,沈昌祥,公备.可信计算 3.0 工程初步[J].网络与信息安全学报,2017,3(9):79.
[3] 陈卫平.可信计算 3.0 在等级保护 2.0 标准体系中的作用研究[J].信息安全研究,2018,4(7):633-638.
[4] 沈昌祥.用主动免疫可信计算构筑新型基础设施网络安全保障体系[J].网信军民融合,2020,35(4):12-15.
[5] 徐意泊,陈富浩,丁振华,等.基于国产龙芯 2K1000 龙芯派的内核系统启动[J].现代信息科技,2018,2(12):29-34.
[6] 王冠.TPCM 及可信平台主板标准[J].中国信息安全,2015(2):66-68.
[7] 易平.基于龙芯处理器的嵌入式可信系统的设计与实现[D].南京:南京航空航天大学,2018.
[8] 易平,庄毅.基于龙芯处理器的嵌入式可信解决方案[J].计算机技术与发展,2018,28(5):112-116.
[9] 张景桢.基于 LINUX 的可信软件基的设计与实现[D].北京:北京工业大学,2017.
[10] 孙瑜,王溢,洪宇,等.可信软件基技术研究及应用[J].信息安全研究,2017,3(4):316-322.
[11] 张家伟.基于 Linux 的可信计算平台研究与实现[D].北京:北京邮电大学,2018.
[12] 周培莹.可信 I/O 资源访问控制策略研究与应用[D].南京:南京理工大学,2009.
[13] 曹喆,王以刚.基于 USBKey 的身份认证机制的研究与实现[J].计算机应用与软件,2011,28(2):284-286.
[14] 于颖超,徐宁,李立新.一种可信增强的访问控制框架的设计与实现[J].电子技术应用,2009,35(1):143-143.
[15] 郭晋.基于可信计算的嵌入式 Linux 内核安全性加固的研究[D].成都:电子科技大学,2011.

(收稿日期:2021-01-29)

作者简介:

孟祥斌(1995-),通信作者,男,硕士,主要研究方向:信息安全、密码学,E-mail:xiangbinmeng@foxmail.com。

刘笑凯(1977-),男,硕士,高级工程师,主要研究方向:信息安全、密码学。

郝克林(1992-),男,硕士,工程师,主要研究方向:信息安全、密码学。

扫码下载电子文档

(上接第 68 页)

ference on Computer Vision & Pattern Recognition,2015.
[5] LI J,ZHAO X,LI H.Method for detecting road pavement damage based on deep learning[C]//SPIE Smart Structures+Nondestructive Evaluation,2019.
[6] 路雪,刘坤,程永翔.一种深度学习的非机动车辆目标检测算法[J].计算机工程与应用,2019,55(8):188-194,220.
[7] Yuan Weiqi,Xue Dan.Overview of detection algorithms for tunnel lining cracks based on machine vision[J].Journal of Instrumentation,2017,38(12):3100-3111.
[8] 阮小丽,王波,荆国强,等.桥梁混凝土结构表面裂缝自动识别技术研究[J].世界桥梁,2017,45(6):55-59.
[9] YANG X C,LI H,YU Y T,et al.Automatic pixel-level crack detection and measurement using fully convolutional network[J].Computer-Aided Civil and Infrastructure Engineering,2018,33(12):1090-1109.
[10] 王森,伍星,张印辉,等.基于深度学习的全卷积网络图像裂缝检测[J].计算机辅助设计与图形学学报,2018,30(5):859-867.
[11] Zhou Ying,Liu Tong.Recognition of concrete cracks based on computer vision[J].Journal of Tongji University(Natural Science),2019,47(9):1277-1285.
[12] 沈新烽,姜平,周根荣.改进 SSD 算法在零部件检测中的应用研究[J].计算机工程与应用,2021,57(7):257-262.
[13] SIMONYAN K,ZISSERMAN A.Very deep convolutional networks for large-scale image recognition[J].arXiv preprint arXiv:1409.1556,2014.
[14] Fu Chengyang,LIU W,RANGA A,et al.DSSD:deconvolutional single shot detector[J].ArXiv abs/1701.06659,2017.
[15] 雷华迪,陈东方,王晓峰.基于级联 SSD 的目标检测算法[J].计算机工程与设计,2020,41(12):225-232.
[16] LIN T Y,GOYAL P,GIRSHICK R,et al.Focal loss for dense object detection[C]//2017 IEEE International Conference on Computer Vision(ICCV).IEEE,2017:2999-3007.
[17] 张琳娜,陈建强,陈晓玲,等.面向行车视频目标实时检测的轻量级 SSD 网络[J].计算机科学,2019,46(7):233-237.
[18] 陈幻杰,王琦琦,杨国威,等.多尺度卷积特征融合的 SSD 目标检测算法[J].计算机科学与探索,2019,13(6):1049-1061.
[19] 蔡逢煌,张岳鑫,黄捷.基于 YOLOv3 与注意力机制的桥梁表面裂痕检测算法[J].模式识别与人工智能,2020,33(10):62-69.

(收稿日期:2021-04-22)

作者简介:

苏可(1995-),男,硕士研究生,主要研究方向:遥感图像处理。

郭学俊(1982-),男,博士,讲师,主要研究方向:遥感图像处理。

陈泽华(1974-),通信作者,女,博士,教授,主要研究方向:智能信息处理和智能控制、粒计算和知识工程、图像处理、区块链、工业大数据,E-mail:zehuachen@163.com。

扫码下载电子文档

版权声明