第34卷 第22期 计 算 机 工 程 2008年11月
Vol.34 No.22 Computer Engineering November 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)22—0239—03 文献标识码：A 中图分类号：TP309

嵌入式终端可信计算环境的关键技术

王震宇[1]，刘鑫杰[1]，任 杰[1]，刘海雷[1]，吴 杰[2]
(1. 解放军信息工程大学信息工程学院，郑州 450002；2. 中国人民解放军九五八七九部队，成都 610081)

摘 要：阐述了在嵌入式终端上构建可信计算环境相关的嵌入式可信引导、TPM的扩展和驱动设计、嵌入式可信软件栈和嵌入式可信安全组件等关键问题。嵌入式可信引导可结合BR, USBKey和TPM等技术，保证用户、终端和应用三者间的可信认证。给出的嵌入式终端可信计算环境的方案保证了嵌入式可信平台的可重用性，同时也使平台具有更高的安全性和实用性。

关键词：嵌入式终端；可信引导；可信软件栈；可信安全组件

Key Technologies for Trusted Computing Environment on Embedded Terminal

WANG Zhen-yu[1], LIU Xin-jie[1], REN Jie[1], LIU Hai-lei[1], WU Jie[2]
(1. Information Engineering Institute, PLA Information Engineering University, Zhengzhou 450002; 2. PLA 95879 Army, Chengdu 610081)

【Abstract】 The paper discusses the key problems to build embedded trusted computing environment, such as embedded trusted boot process, the extension and driver design of TPM, embedded TSS and trusted security component. The embedded trusted boot process is able to ensure the trusted attestation among users, terminals and application by making a combination of BR, USBKey and TPM. The scheme is able to make embedded platform more secure, practical and reusable.

【Key words】 embedded terminal; trusted boot; trusted software stack; trusted security component

1 概述

随着全球信息化的飞速发展，信息安全问题备受关注。现今利用各种安全技术手段如防火墙、入侵检测和杀毒软件来实现安全防护，使得整个信息系统级安全保障变得更加复杂，系统维护与管理复杂度与成本不断提高，同时还使得使用效率大大降低。此种状况的一个重要原因为忽略了终端安全的有效保护[1]。终端作为保存重要数据的源头，数据泄密和病毒感染也往往由于终端脆弱性引起，从另一个角度来说，在网络上大多数攻击事件基本上都由终端发起。如果采用可信终端，将非安全因素在终端进行过滤，使得终端上的每一个操作都是可信的行为，就能够更好地保证整个信息系统的安全。随着嵌入式终端在数据服务或货币支付等领域的广泛应用，对其安全性的要求也越来越高，构建一个嵌入式终端的可信环境的需求显得越来越迫切。

可信计算联盟(Trusted Computing Platform Alliance, TCPA)于2001年发布了TCPA v1.1标准规范。2003年TCPA改组为可信计算组织(Trusted Computing Group, TCG)并于2004年颁布了1.2版本的规范。同年，TCG将可信计算的思想引入到移动终端，提出了可信移动平台(TMP)的软、硬件体系和协议3个技术标准草案，用以提供端到端的安全移动计算环境。ARM公司在嵌入式平台上给出了可信计算技术的解决方案——TrustZone。TrustZone由硬件增强的安全性环境(提供代码隔离)与安全软件组成，安全软件提供基础安全服务和与信任链中其他单元的接口，包括智能卡、操作系统和一般的应用程序。TrustZone将两个并行的执行领域分隔开：没有安全性要求的“正常”执行区域和可信任的、可认证的安全区域。但是，TMP规范是框架性的指导，并未规定具体构建可信嵌入式平台的实施方案；而TrustZone等技术尚未成熟和产业化。

2 相关工作背景

Arbaugh提出的AEGIS体系结构在FreeBSD系统上实现了一个安全引导的原型系统[2]，它将系统引导过程分为5个层次，控制权在层间进行传递。通过层间的完整性验证来确保引导过程的安全。

IBM基于TCG规范在Linux系统下实现了一个完整性度量的体系架构[3]。通过修改Linux系统，在操作系统和上层应用加载运行前对其进行完整性验证，从而将TCG规范中的信任关系从BIOS层延伸到了应用程序层。

文献[4]提出了一种基于可信服务器的可信引导的实现。在OS引导过程中，信任的传递从MBR开始。从MBR开始往后的3个阶段建立可信链：MBR，OS装载程序，操作系统内核。在可信链的建立过程中，需要与可信服务器进行交互，以进行验证码的验证。

文献[2]中所定义的结构同TCG所定义的可信引导过程类似。但没有涉及如何计算验证实体的预期完整性值问题，因此该可信引导过程并不完整。作为一个原型系统，其思想值得借鉴。文献[3-4]分别从PC和服务器2个角度设计了TCG规范下的可信引导方案。而OpenTC的TrustedGRUB做为开放源码的PC可信引导实例，为嵌入式终端平台的可信引导

基金项目：国家“863”计划基金资助项目(2007AA01Z483)
作者简介：王震宇(1969－)，男，副教授、博士研究生，主研方向：可信计算，信息安全，计算机体系结构；刘鑫杰、任 杰、刘海雷，硕士；吴 杰，助理工程师
收稿日期：2008-06-24 **E-mail：**wzyzw2008@yahoo.com.cn

提供了参考。

另外，值得关注的还有由微软提出的“下一代可信计算基”(NGSCB)计划和英特尔公司提出的 LaGrande 技术(LT)，由于其在业界的影响力，这 2 个计划代表了未来可信计算 PC 平台事实上的工业标准。

3 基于 ARM 的嵌入式可信终端硬件构成

本文所构建的基于ARM的嵌入式终端基本硬件环境是基于ARM9 以上的内核。ARM9 以上内核的微处理器的基本硬件资源通常含有独立的指令和数据缓存用于虚拟内存管理MMU单元、系统管理器(包括片选逻辑控制和SDRAM控制器)、异步串口(UART)、DMA、脉宽调制(PWM)的定时器、实时时钟单元、IIC总线接口、SMBus总线接口、USB设备接口、SPI接口和锁相环(PLL)时钟发生单元、LCD控制器(STN&TFT)、10 M/100 M网口[5]。

为了使嵌入式终端的硬件资源满足可信计算的要求、增强终端系统的安全性，需要在基本的硬件环境之上做以下硬件配置：

(1)TPM 芯片扩展

在嵌入式终端平台上可以通过 SMBus 等总线外扩 TPM 芯片(选择 ATMEL 的 AT97SC3203S)。TPM 通过 DMA 方式访问 USBkey、生物特征读取设备。

(2)使用 USBKey

将用户信息存放在 USBkey 中，使用 USBkey 可以提供诸如身份认证、电子签名、权限管理等诸多安全功能。另外嵌入式可信终端利用 TPM 和 USBkey 的绑定进行用户的身份认证，对 USBkey 的认证是通过安全模块 TPM 实现的，从而提高了用户身份的安全级别。

(3)生物特征认证

在终端平台上利用高速 UART 接口外接生物特征读取设备(Biometric Reader, BR)。选用较为通用的指纹采集仪，使用生物认证技术来增加身份认证的安全性和激活存储密钥。

图 1 描述了以 ARM 处理器核为基础构建的可信终端硬件框架。TPM、UART 接口、USB 接口和 LCD 控制器可以共享 DMA 控制器，也可使用不同的 DMA 通道分时占用系统总线。TPM 既可利用 DMA 接口直接访问 SRAM，也可通过局部 I/O 总线与 BR 传送数据。BR 通过 UART 接口与处理器核相连。

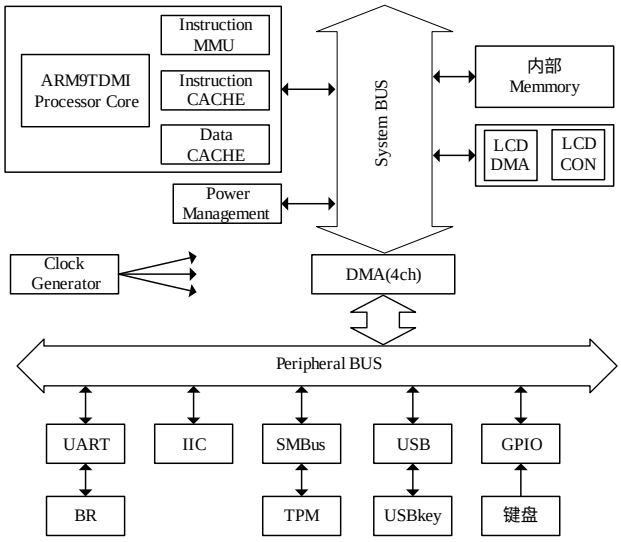

图 1 可信终端功能框图

4 构建嵌入式可信终端环境关键技术

TPM 芯片作为终端平台提供可信支撑的基础部件，可以通过 SMBus 等总线物理嵌入到平台上，同终端平台逻辑绑定，形成一一对应关系。由配置程序生成一对内外部认证密钥(也可采用证书系统来建立绑定关系)。另一方面，USBKey 作为移动设备用于用户身份认证，必须为其建立合法持有者；BR 的使用可以增加用户身份认证的安全性。嵌入式可信终端可信环境的构成着重于从体系结构上将安全功能和可信机制结合起来，有效保障安全策略正确实施，确保平台基础可信和总体安全目标的实现。

在构建终端可信环境过程中，可信引导机制和嵌入式可信软件栈是可信终端平台的重要组成部分。可信引导作为平台总体安全基础，对操作系统装载器、OS 内核、硬件配置信息等进行验证，确保引导过程中各部件的完整性，使平台按照经过严格验证的方式进行引导；嵌入式可信软件栈为终端平台使用 TPM 提供统一接口的同时，也为平台上层的安全应用提供基础。

4.1 可信引导

嵌入式系统中，系统引导(BootLoader)的作用与 PC 上的 BIOS 类似，通过引导程序可以完成对系统平台的主要部件的初始化工作。但是嵌入式系统的资源远远没有 PC 的资源丰富。本文所构建的嵌入式终端系统在加电时，除了完成终端系统必须的初始化工作之外，还要为 TPM 芯片的使用建立可执行环境。与现有的嵌入式终端引导相比，本文提出的可信终端框架的硬件构成由 BR 模块、USBkey 模块配合 TPM 一起完成可信引导工作。将可信引导的整体工作分为 2 个阶段。

4.1.1 阶段一操作

完成基本硬件初始化(包括 TPM)；度量阶段二的代码，并将度量结果存储；准备 RAM 空间并将可信引导阶段二的代码拷贝进去；设置堆栈指针；最后跳转到阶段二的 C 入口点。在 TPM 的初始化过程中需要完成以下工作：激活 SMBus 总线，使能 TPM 芯片，为 TPM 分配 I/O 地址，配置并初始化 TPM。阶段一是可信引导一开始就执行的操作，其目的是建立可信环境的执行基础，并为引导工作第二阶段的执行以及随后的内核的执行准备好基本的硬件环境。

在可信引导的阶段一中，由于硬件资源限制只能使用 TPM 的最小功能集来完成可信计算的工作。其主要完成的工作如下：

(1)初始化 TPM，建立并验证 TPM 设备同驱动之间的通信流。

(2)对 Platform Configuration Register(PCR)执行 TPM_SHA1Start, TPM_SHA1Update 与 PM_SHA1CompleteExtend 操作，完成 hash 操作；将缓冲区中的数据传输到 TPM 并读取 TPM 的响应值。

(3)通过 bPhyPresenceTPMCmdId 参数的设定，与 TPM 通信。

4.1.2 阶段二操作

初始化本阶段要使用的硬件设备；检测系统的内存映射；检测和加载内核映像和根文件系统映像并设置内核的启动参数，最后调用内核。阶段二要完成串口、GPIO 和 USB 接口的初始化；对操作系统镜像进行度量；在此过程中 TPM 通过 DMA 方式访问 USBkey 和 BR；然后执行内核镜像校验，通过后将控制权移交，最终完成可信引导。

可信终端加电后，首先插入 USBKey 验证平台的合法性。

USBKey 负责存储用户的数字证书和敏感信息，如认证参数、指纹模板等。只有在确认平台当前状态可信之后，用户才通过键盘输入口令，并利用 BR 提供自己的指纹，以防止用户的敏感信息被恶意终端窃取，达到可信引导的目的。

4.1.3 TPM 驱动

TPM 的初始化和驱动加载是可信引导的关键技术点。可信引导过程中将关键数据存储到 TPM 内部的 PCR(Platform Configuration Register)寄存器。PCR 属于易失性存储，目前 TPM 支持 16 个，每次开机时均复位零。伴随系统的启动和控制权的逐级传递，采用 TPM 提供的 Shal 度量各个模块保存完整性值，同时调用 TPM 内部命令 Extend 把度量结果写入相应 PCR。Extend 操作把当前 PCR 值和新计算的值进行链接后再调用 Shal，用输出的值更新 PCR，实时准确地记录系统的状态信息，防止伪造度量列表项的数据。

阶段二中通过加载TPM驱动可以对TPM执行更多的操作[6]。在阶段一中TPM完成初始化工作，接着TPM会在其成功地完成自检(self-tests)之后才允许TPM芯片进入全功能操作状态。直到为TPM建立一个拥有者(TPM owner)，才能全部实现TPM的功能。具体实现过程如图 2 所示。

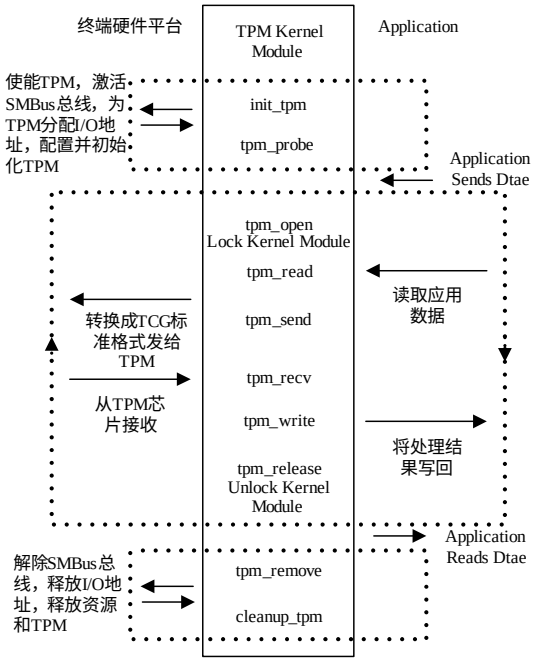

图 2 TPM 驱动执行

TPM_open 为应用者提供一个访问 TPM 的接口，但是在一个应用调用 TPM_open 之后 TPM 就工作在单工状态。在此过程中只允许一个进程访问 TPM，驱动程序将该进程的操作和数据转换成 TCG 的标准发给 TPM 并将 TPM 的处理结果转换后返回给该进程。

4.2 嵌入式 TSS

TCG Software Stack(TSS)[7]是支持 TPM平台的支撑软件，它规定了TPM与操作系统结合的方式和接口。

TSS 简化了使用 TPM 的复杂性，开发者只需要了解 TPM 的基本概念和 TSS 向上层提供的接口，就可以很容易在嵌入式可信终端平台上开发基于 TPM 的安全应用程序。

TSS 主要由 TCG 服务提供层、TCG 核心服务层、可信设备驱动库函数层和可信设备驱动层 4 大模块组成。其各层功能在此不再赘述。如图 3 所示。

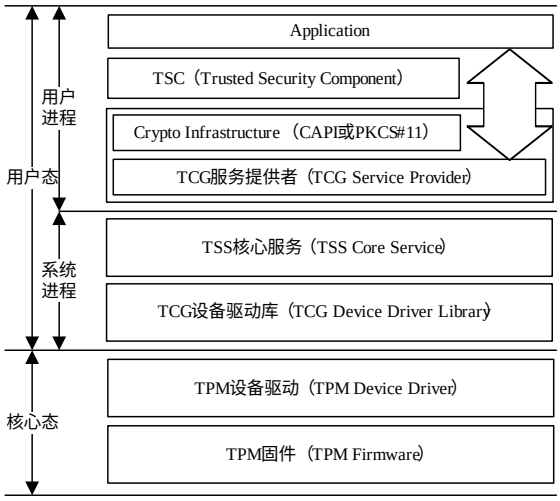

图 3 嵌入式可信终端软件栈结构

在本案的设计中，将 TSP 层分为 6 个功能模块。它们分别是 TSP 接口模块、命令参数组包模块、密钥管理模块、加密模块、对象管理模块、会话模块和 TSP 命令接口模块。其中，加密模块的功能可使用 RSA 的 PKCS#11 或 MicmsoR 的 CryptoAPI 加密接口规范实现。

在嵌入式终端上对 TPM 的调用有着特殊的安全应用。本案的嵌入式可信终端应用中，在 TSP 层之上增加 TCS(Trusted Security Component)。与传统的 TSS 软件栈使用相比，TCS 层将 TSP 层的功能进行封装，可以简化嵌入式可信终端的可信组件和其他应用程序的开发工作，提高工作效率，还可以增加在平台上软件使用的安全性，另外还方便了针对嵌入式终端平台的代码移植。TCS 层将基于嵌入式可信终端软件栈和可信机制提供可信计算规范中所要求的完整性度量、完整性报告、密钥管理、密码服务、密封存储(sealed storage)保护存储(protected storage)和远程证言(remote attestation)等可信安全组件。使用 TCS 可以提高二次开发的效率和软件的可重用性。下面主要描述 TSP 层 3 个模块的基础组织结构，如图 4 所示。

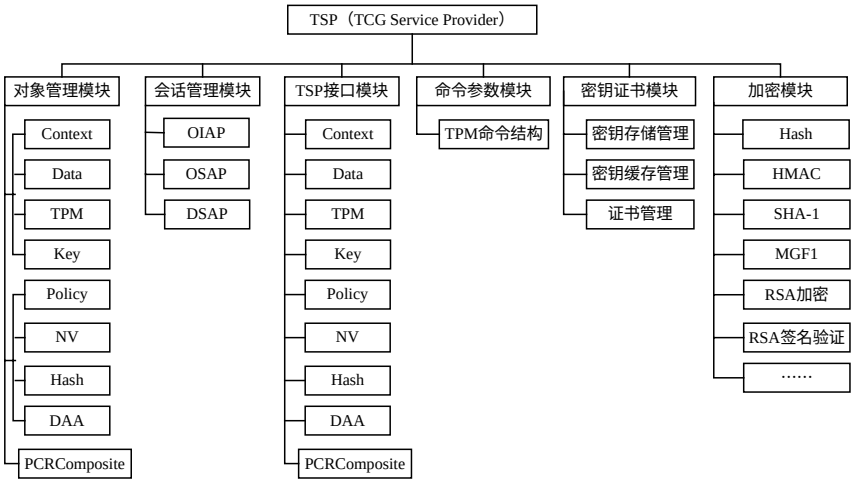

图 4 TSP 基础组织结构

(下转第 244 页)