计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(7): 1269-1278, 2011

嵌入式系统可信平台模块研究

张焕国　李　晶　潘丹铃　赵　波
[1](武汉大学计算机学院　武汉　430072)
[2](空天信息安全与可信计算教育部重点实验室(武汉大学)　武汉　430072)
(lijing-whu@163.com)

Trusted Platform Module in Embedded System

Zhang Huanguo, Li Jing, Pan Danling, and Zhao Bo
(*School of Computer, Science, Wuhan University, Wuhan* 430072)
(*Key Laboratory of Aerospace Information Security and Trust Computing* (*Wuhan University*), *Ministry of Education*, *Wuhan* 430072)

Abstract　How to effectively enhance the security of embedded system is an issue that is difficult to tackle and it attracts much attention in the field of information security. Relative research shows that trusted platform module (TPM) plays a crucial role in efficiently enhancing the security of information system. However, existing TPM is designed for PCs, and thus cannot satisfy the specific application needs of embedded systems. Addressing this issue, we analyze the challenges in the research of TPM posed by the embedded system environment, and propose a novel embedded trusted platform module (ETPM) that can adapt to such environment. As important components in ETPM, bus arbitration improves the platform's control ability and increases the security of embedded system; symmetric cryptography engine accelerates the speed of symmetric encryption and decryption; and system backup-recovery enhances the reliability of the embedded system. Furthermore, ETPM supports star style measurement module in embedded system environment. ETPM has been tested in trusted PDA, and experiment results show that ETPM is practical, efficient, reliable and secure.

Key words　information security; trusted computing; embedded system; trusted platform module; embedded trusted platform module

摘　要　如何有效增强嵌入式系统的安全性是信息安全领域研究的热点和难点之一.相关研究表明,可信平台模块对于有效提高信息系统的安全性十分重要.然而,现有的可信平台模块是为个人计算机设计的,并不能满足嵌入式系统特有的应用需求.针对上述问题,设计了一种适应嵌入式环境的新型嵌入式可信平台模块(embedded trusted platform module, ETPM).作为嵌入式可信平台模块的重要组成部分,总线仲裁提高了ETPM的控制能力,增强了嵌入式系统的安全性;对称密码引擎提高了嵌入式系统的对称密码运算效率;系统备份恢复增强了嵌入式系统的可靠性.除此之外,ETPM还能够支持嵌入式平台的星型信任度量模型.这一设计已经在可信PDA中进行了实验验证,实验表明嵌入式可信平台模块是实用、高效、可靠、安全的.

关键词　信息安全;可信计算;嵌入式系统;可信平台模块;嵌入式系统可信平台模块

中图法分类号　TP309

收稿日期:2010-09-01;**修回日期**:2010-12-22

基金项目:国家自然科学基金项目(60970115,61003268,91018008);湖北省自然科学基金重点项目(2009429);中央高校基本科研业务费专项基金项目(3101038);武汉大学国防培育基金项目(29)

随着信息化发展,嵌入式系统得到了最为广泛的应用.小到电子手表、家用电器、自助取款机,大到汽车、火车、飞机、火箭,嵌入式系统已经深入到经济、教育、科技和军事的方方面面.

在金融领域,嵌入式系统上运行的程序往往与用户的货币相关;在军事领域,高科技武器中的嵌入式系统安全性很可能决定着一场战争的胜负.由此可见,嵌入式系统的安全至关重要.

信息安全领域的研究中,硬件结构和操作系统的安全是信息系统安全的基础,而密码、网络安全等是其关键技术.只有从信息系统的硬件和软件的底层采取安全措施,才能比较有效地确保信息系统的安全[1].因此,要解决嵌入式系统安全问题,近年兴起的可信计算技术是一个行之有效的办法,其主要思路是建立可信根和信任链来保证系统的完整性和安全性.

目前,可信计算组织(Trusted Computing Group, TCG)已经提出了用于解决移动平台的安全规范[2-3]和设想;国内的一些学者[4-7]也提出了利用TCG规范的可信平台模块(trusted platform module, TPM)与嵌入式CPU进行通信,以改善嵌入式系统安全水平的方法.但是,这些方案都是基于传统的TPM,该模块是针对PC计算平台设计的,并不能满足嵌入式平台特有的应用需求,也没有解决TPM与嵌入式系统CPU共存时对系统的控制问题[8].

本文首先分析嵌入式系统环境对可信平台模块研究的新挑战,然后针对这些挑战设计一种嵌入式环境下的TPM,最后通过实际系统的应用,分析其特点,并证明这种新型的TPM是实用、高效、可靠、安全的.

1 嵌入式环境下TPM面临的新挑战

目前,在通用计算机领域,TCG已经制定了可信计算平台模块的规范.该规范规定了其逻辑结构[9]、功能以及对可信计算机制的支持.除此之外,众多学者也对TPM结构进行了深入的研究,并且提出了一些新的TPM架构[10-13],这些研究在一些方面弥补了TCG标准中TPM的缺陷.

但是,与通用计算机平台相比,嵌入式系统具备自身的一些特点:以应用为中心,嵌入式系统往往有特定应用场景;硬件设计自由,嵌入式系统的硬件往往可以自主设计;系统软、硬件设计灵活,具有可裁剪性;嵌入式系统往往对功能、可靠性、成本、体积、功耗等有严格要求.

由此可见,嵌入式系统的不断发展,为可信平台模块的研究提出了新的挑战.

1) TPM芯片缺乏主动控制能力

TPM作为一个信息安全芯片,通过主板接口与主机相连,或者直接固化到主板上,作为可信平台的信任根.然而在实际使用中,出于对现有系统的迁就,TPM往往通过特定接口插在主板上,被当作计算平台的一个从设备来使用,它相当于计算机中的一个安全协处理器,当主机需要安全服务时,由TPM提供这种服务.而主机如果不向TPM要求这些服务,TPM就不能参与平台的安全管理工作.

由于通用PC的处理器具有较强的处理、调度能力,传统的TPM作为协处理器即可适应其安全需求.但是,嵌入式系统中的处理器调度能力往往相对较弱,无法进行复杂的调度与分配,难以控制整个信任链的度量与扩展过程.

与此同时,嵌入式系统具有软硬件可裁剪性,在系统研发和使用的过程中,极有可能根据实际环境对其上的软、硬件进行改动,去除其中部分不需要的模块或者增加一些必要模块.这些改动,都需要经过可信嵌入式平台的完整性度量,这无疑加重了处理能力本就较弱的嵌入式处理器的负担.若嵌入式系统中的TPM具有更好的控制能力,能够控制嵌入式平台的信任链扩展过程,将会对可信嵌入式系统的效率和灵活性起到较大帮助.

因此,嵌入式系统灵活多变的环境与TPM主控能力之间的矛盾,激发了对嵌入式系统TPM的新挑战:该环境下的TPM,需要增强自身对平台的控制能力,从通用PC机中的协处理器,转变为一个主控设备,控制嵌入式系统信任链的度量与扩展,这也正符合了TCG提出的TPM作为可信平台主控,确保平台安全的初衷.

2) 密码机制存在不足

TCG规范在TPM的结构中没有明确设置对称密码.TCG在规范中一方面说允许采用对称密码,可另一方面又多次强调淡化对称密码.众所周知,公钥密码和对称密码各有自己的优缺点,在应用中同时采用这2种密码互相配合,才能发挥更好的安全作用.而TCG在TPM中只设置公钥密码引擎,不设置对称密码引擎,显然有不足之处.并且,TCG在TPM结构中没有设置对称密码引擎,但在密钥设置时却设置了对称密码密钥.因此,用户只能采用软件方式实现对称密码,这必然导致对称密码

的加解密速度不高.

另外,TPM 密钥种类繁多,管理复杂. TCG 采用如此繁多的密钥的主要原因是在 TPM 中采用了公钥密码 RSA,而没有采用对称密码,使得采用公钥密码和对称密码结合很容易解决的问题,若只采用公钥密码就必然要麻烦得多.

在通用 PC 机中,因为其运算速度快,处理能力强,不管是使用软件实现对称密码加解密或者使用种类繁多的 TPM 密钥,都不会严重影响平台的正常运行. 但是,嵌入式系统往往对效率有着极高的要求,再加上嵌入式处理器的运算能力往往较低,使用软件实现对称密码加解密将影响其实时性,严重影响嵌入式系统的效率.

因此,嵌入式系统对传统 TPM 提出了又一需求:嵌入式系统可信平台模块需要具备硬件加解密引擎,提高密码运算效率.

近年来,随着可信计算技术的发展与应用,特别是在了解了中国可信计算的发展后,TCG 也逐渐认识到在 TPM 设计方面存在的不足. 于是,TCG 开始制定 TPM 的新规范,并命名为 TPM. next[14-15]. TPM. next 吸收了中国可信密码模块(trusted cryptography module,TCM)的长处,使 TPM 更加灵活,并且增加了对 PC 机和服务器的支持. 但是,该规范仍然对嵌入式系统中的 TPM 欠缺考虑.

综上所述,嵌入式系统的自身特点,对 TPM 研究提出了新的挑战. 有必要研究一种新型 TPM,这种 TPM 除了具备 TCG 规范中的基本功能之外,还应该具备一些新的功能与特性,符合嵌入式环境下的特殊需求.

2 嵌入式系统可信平台模块

针对嵌入式系统的特点,本文设计了一种嵌入式系统可信平台模块(embedded trusted platform module, ETPM),ETPM 在传统 TPM 的基础上作了一些改进,不仅应对了嵌入式系统对 TPM 研究提出的新挑战,还增强了嵌入式系统的可靠性,并且作为信任根为嵌入式系统上星型信任度量模型[16]提供了支撑,有效减少了信任传递过程中的信任损失. ETPM 逻辑结构如图 1 所示.

本设计在原有 TPM 的基础上,新增了总线仲裁模块、对称密码引擎和备份恢复模块. 其中,总线仲裁模块用于提高 ETPM 的控制能力;对称密码引擎提供对称密码的硬件加解密功能;备份恢复模块提高了整个系统的可靠性.

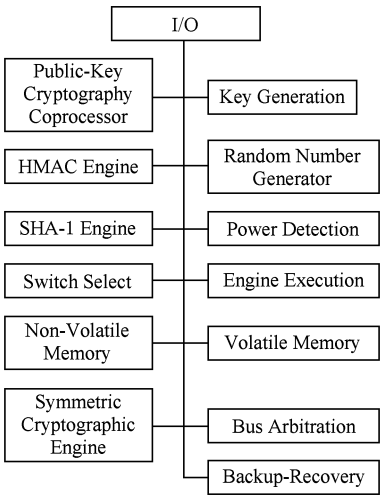


Fig. 1 Logical structure of ETPM.

图 1 ETPM 逻辑结构

2.1 总线仲裁

可信计算平台中,TPM 的引入带来 2 个问题:一是启动流程,在上电后,TPM 必须先进行完整性检验,此时平台处理器和外设还不能启动,在 TPM 校验通过后,才能允许平台处理器和外设启动;二是 TPM 与平台处理器都要读取外部存储器的数据,这就存在一个对存储器的互斥访问问题.

传统 PC 机的处理器调度能力较强,以上 2 个问题由 CPU 控制解决. 而嵌入式系统的处理器调度能力较弱,整个信任链扩展过程需要由 TPM 控制执行. 针对这种需求,本文将总线仲裁模块加入到 ETPM 的设计中,主要负责嵌入式系统的启动控制和存储器的互斥访问. 其工作方式如图 2:

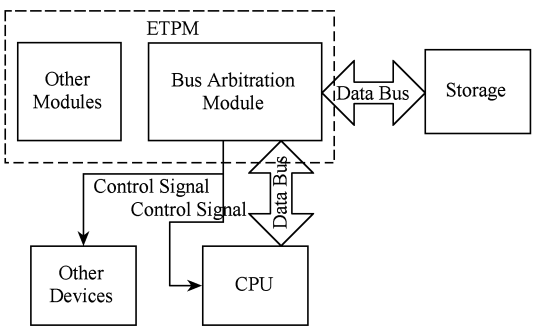


Fig. 2 ETPM bus arbitration module.

图 2 ETPM 总线仲裁模块

本设计中,ETPM 处于核心地位,总线仲裁模块对外部存储器总线控制权进行仲裁,并对嵌入式系统进行控制. 基于上述结构的总线仲裁模块可以完成启动控制和系统仲裁的功能.

为了便于进行启动控制和总线仲裁,我们在 ETPM 中定义了 2 个寄存器:控制寄存器、状态寄存器.

1) 控制寄存器(CR)

7	6	5	4	3	2	1	0

其中,

0:复位信号,低有效;

1:嵌入式系统启动;

2:仲裁信号 ;

3:读外部存储器开始;

4:校验完成;

5:写外部存储器开始;

6:启动失败.

2) 状态寄存器(SR)

7	6	5	4	3	2	1	0

其中,

0:校验数据准备好;

1:完成读外部存储器;

2:校验开始;

3:写外部存储器完成;

4,5,6,7:保留.

注:以上所有寄存器位除复位信号外,都是高有效.

ETPM 启动控制与总线仲裁方法如下.

启动控制: 以 ETPM 中的控制寄存器 CR 的 0 位为硬件控制信号,该控制信号与 CPU 及主板其他设备相连,通过使能该信号能够使 CPU 处于重启状态无法工作,并可以使其他设备处于 unable 状态. 因此,在系统启动初期,ETPM 正常工作,并使 CPU 和主板其他设备无法启动,从而确保了可信平台的启动流程.

总线仲裁:外部存储器和 CPU 均通过数据总线连接到 ETPM 的总线仲裁模块中,ETPM 启动之后,置仲裁位 *CR*[2]为 1,总线仲裁模块首先获取外部存储器总线占有权,并将其连接到 ETPM 中,ETPM 置 *CR*[3]为 1,开始读取外部存储器,若 *SR*[2]为 1,ETPM 则开始对获取的数据进行完整性校验. 若完整性校验通过(*CR*[4]为 1),则 *CR*[2]为 0,*CR*[1]为 1,使总线仲裁模块释放总线,并将 CPU 数据总线与系统总线相连接,使嵌入式系统拥有总线占有权. 若完整性校验不通过,ETPM 将自动调用备份恢复模块,进行系统恢复.

ETPM 控制下的可信平台系统启动状态如图 3 所示:

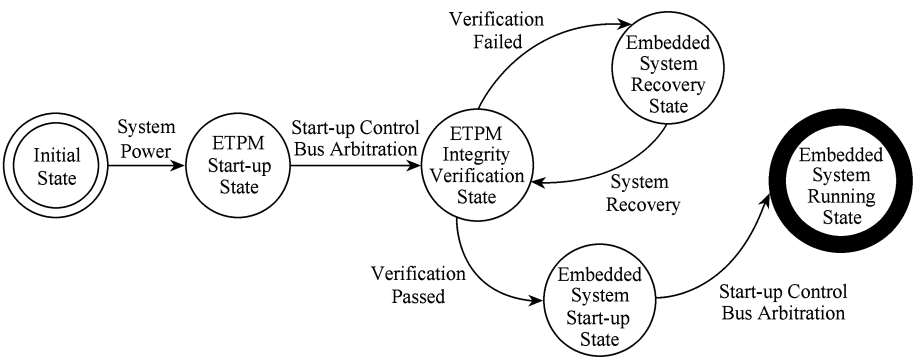


Fig. 3 Trusted Platform boot state diagram.

图 3 可信平台启动状态图

总线仲裁模块的引入,使 ETPM 得以突破传统 TPM 的限制,成为主设备控制计算机系统,使系统具有良好的扩展性. 同时,平台启动控制、完整性度量、系统总线互斥访问和外设控制等功能都得以直接由 ETPM 完成,而无需其他部件参与,更为安全、可靠.

因此,该设计使得 ETPM 更符合嵌入式系统灵活多变的环境,并且解决了嵌入式系统 CPU 与 TPM 共存时对系统的控制问题.

2.2 备份恢复

根据"可信≈可靠+安全"的学术思想[17-18], ETPM 中加入了独有的备份恢复模块,该模块提高了整个可信计算平台的可靠性. 在系统被非法更改之后,ETPM 的备份恢复模块会在系统启动时进行检测,发现异常立即将系统关键数据恢复,防止系统被篡改.

本文对 TCG 规范所规定的 TPM 结构进行了扩展,在 ETPM 内部添加一个受物理保护的系统备份存储器,将平台引导程序和部分操作系统关键数据存储在内. ETPM 在可信平台启动之前对其引导程序代码和部分操作系统关键代码进行完整性校验,若校验未通过则认为以上内容被篡改, ETPM 使用总线仲裁机制获取总线控制权,并从受保护的

备份存储器中读取标准可执行代码,将其写入平台外部工作用存储器,在写入后将再次进行完整性校验,若通过校验,表明系统恢复成功,ETPM 将交出总线控制权,允许计算机系统启动.

ETPM 备份恢复如图 4 所示:

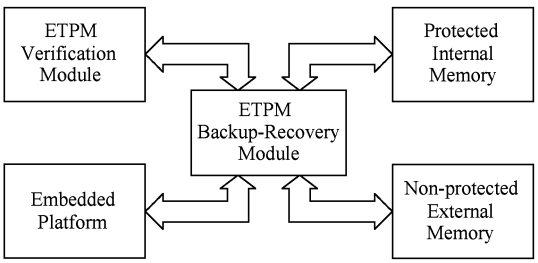


Fig. 4 ETPM system backup and recovery.

图 4 ETPM 系统备份恢复

ETPM 备份恢复能力的引入,增强了平台的持续工作能力和抗篡改能力.与现有的技术相比,该方式还有如下优点:由 ETPM 作为系统的可信根,对可执行代码进行完整性校验,同时为备份存储器提供受保护的安全存储环境.ETPM 拥有计算机总线控制权,在进行完整性校验和系统恢复的过程中不会受到外部干扰.

2.3 对称密码引擎

为了满足嵌入式系统对称加解密的需求,本文在 ETPM 内部设计了硬件对称密码引擎,通过可信软件栈(TCG software stack, TSS)为上层应用提供对称密码加解密服务.这使得 ETPM 中同时具备对称密码和非对称密码加解密能力,从而在 ETPM 使用过程中,得以将这 2 种密码互相配合,发挥出更好的安全作用,也弥补了原有 TPM 中只设置了非对称密码,却没设置对称密码所引起的不便.

本设计使用 SMS4 对称密码算法.该算法是 2006 年 1 月我国官方公布的第 1 个商用密码算法.该算法是一个迭代型分组算法,分组长度为 128 b,密钥长度也为 128 b.加密算法与密钥扩展算法都采用 32 轮非线性迭代结构.解密算法与加密算法的结构相同,只是轮密钥的使用顺序相反,解密轮密钥是加密轮密钥的逆序.

根据嵌入式系统的工作要求和 SMS4 算法的特性,加密引擎的设计分为 3 个模块:系统接口模块,缓冲区模块,密码算法模块.

系统接口模块是嵌入式系统与加密引擎通信的桥梁.嵌入式系统与加密引擎的通信通过对加密引擎中的寄存器操作实现,而对这些寄存器的操作则在系统接口模块中实现.主要的寄存器包括:控制寄存器、状态寄存器、输入数据寄存器、输出数据寄存器.

缓冲区模块可以屏蔽系统传输速度与密码算法模块处理速度的差异,提高加解密效率.输入缓冲区将系统输入的密钥或加解密数据进行缓冲,可以使系统数据传输与加解密操作同步进行;输出缓冲区将加解密后的数据进行缓冲.

密码算法模块使用硬件实现标准 SMS4 算法.该算法为分组密码算法,容易硬件实现,并且具备较高的运算速度.

ETPM 的对称密码引擎支持硬件加解密,具有方便灵活、运算速度快的优点.

总线仲裁能力、对称密码引擎和系统备份恢复能力的增加,将使 ETPM 更符合嵌入式系统环境.除此之外,ETPM 还具备传统 TPM 的所有功能:ETPM 内部包含执行引擎、存储器、I/O、2048 位 RSA 密码引擎、随机数产生器等部件.可以很好地完成加密、签名、认证、密钥产生等安全功能.

3 ETPM 星型度量模型

在可信计算平台中,系统的启动要通过完整性校验,即可信根 TPM 对平台进行完整性度量,只有 TPM 认为是安全可靠时系统才能启动.不同的度量方式称为不同的信任度量模型.ETPM 的设计,使得 ETPM 不仅能够支持 TCG 定义的传统链式信任度量模型,更能够对星型信任度量模型[16]提供有力支撑.

3.1 链式信任度量模型

根据 TCG 规范中的定义,信任传递呈一种链式结构,在可信平台的信任链传递过程中,各层可信代理之间层层传递信任关系[19].链式信任度量模型如图 5 所示,从根节点开始,一级度量一级,一级信任一级.

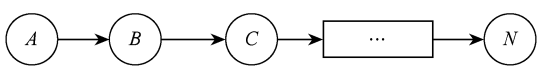


Fig. 5 Chain style trust measurement model.

图 5 链式信任度量模型

现有 PC 机使用链式信任度量模型的主要原因:一方面是因为这种信任度量模型易于工程实现;另一方面是受到现有计算机结构的局限,从 BIOS 到操作系统加载器(OS Loader),到操作系统,再到应用,是一个链式关系,很容易从信任根出发,一级

一级往下信任,从而达到整体可信.

虽然 TCG 的链式信任度量模型使用广泛,但是该结构仍然存在一些不足之处[16]:1)由于可信的测量值采用迭代的计算方法,因此如果在信任链形成后增加或者删除部件,或者软件系统的升级更新,都必须重新计算所有的信任值,增加了维护和管理的难度,这使得该信任度量模型不适应嵌入式系统灵活多变的环境;2)根据信任理论,信任值在传递过程中都会有损耗,传递的路径越长,则损耗越大.因此链式信任度量模型容易出现信任强度减弱和平台常规工作效率下降等问题.

3.2 星型信任度量模型

链式信任度量模型增加、删除部件不灵活,并且在信任传递过程中可能会产生信任损失,这显然与嵌入式系统的高灵活性相违背,一定程度上阻碍了可信计算技术在嵌入式系统环境下的发展.为了解决这些问题,一个好的解决方法是引入星型信任度量模型,即系统各部件均由 TPM 进行校验,通过后才让系统启动.

星型信任度量模型如图 6 所示:

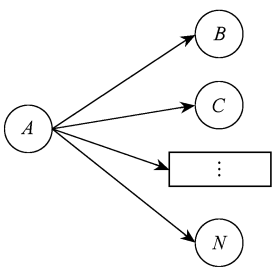


Fig. 6 Star style trust measurement model.

图 6 星型信任度量模型

星型信任度量模型各节点均由根节点进行度量,在信任链扩展过程中,不依赖于前一节点,当有新节点加入,或者有部分节点删除时,只需由根节点进行度量即可,而不需重新度量整个信任链.同时,由于所有节点直接与根节点联系,不存在过多的信任传递过程,由信任传递引起的信任损耗将大大减小.由此可知,星型信任度量模型能有效降低信任损失,提高信任链灵活扩展能力.

与 PC 相比,嵌入式系统具备灵活且易于修改的结构特点,并且其引导程序、内核和根文件系统常存储于同一块存储介质中,对 TPM 而言是并列关系.因此,星型信任扩展方式在嵌入式系统中更容易实现.

星型信任度量模型也有不足之处:在星型结构中,根节点处于中心位置,节点的增加、删除以及使用都受到根节点的控制,增加了节点负担.对应到可信计算平台,TPM 作为根节点,在平台的工作过程中需要不断地对各节点进行完整性度量和可信度的判断,因此,星型信任度量模型的引入,增加了 TPM 在平台控制和计算能力方面的要求.

3.3 ETPM 星型度量模型

ETPM 在控制能力和计算能力方面的增强,正满足了星型信任度量模型对 TPM 的需求.ETPM 的设计与实现,为实现嵌入式系统环境下的星型信任度量模型提供了有力支撑.

ETPM 信任度量模型见图 7:

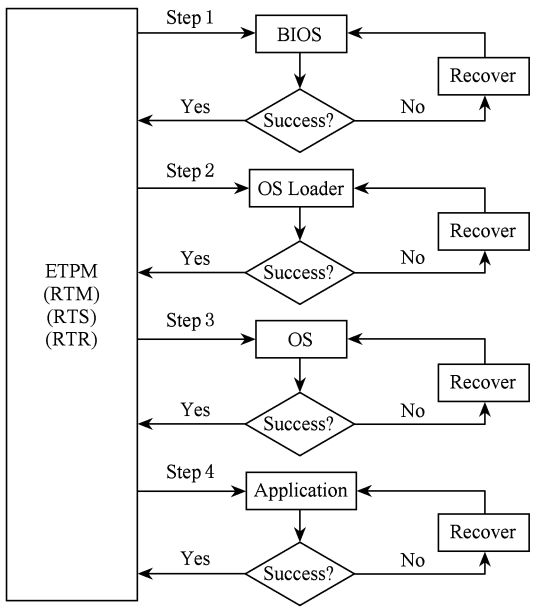


Fig. 7 ETPM star style measurement model.

图 7 ETPM 星型度量模型

与 TCG 的链式信任度量模型相比,该模型具有以下优点:

1) ETPM 内部采用物理方式集成有可信计算根(root of trust for measurement, RTM)、可信存储根(root of trust for storage, RTS)和可信报告根(root of trust for report, RTR),对其自身以及连接电路有良好的物理保护,相较传统的软件实现 RTM 安全性更高;

2) ETPM 的启动控制与总线仲裁能力,使 ETPM 对系统各部件分别校验成为可能;

3) ETPM 的备份恢复能力,有效增强了系统的可靠性;

4) RTM 到任何一个被测量部件都是一级测量,没有多级信任传递,信任损失少;

5) ETPM 对任何部件的测量不依赖于其他部件,具有良好的可扩展性与灵活性,更适合嵌入式系统.

由此可见,ETPM 的设计,是嵌入式平台下的星型信任度量模型的核心,是可信嵌入式系统不可或缺的一部分.

4 实例分析

目前,我们已经设计出 ETPM 的实验系统,并将其作为嵌入式系统的可信根,在可信 PDA 中进行了实验验证.

4.1 ETPM 实例

在 ETPM 的搭建过程中,由于受到现有实验条件的制约,我们无法制作 ETPM 芯片,因此我们使用了一块 FPGA 与密码芯片相结合,完成 ETPM 设计的功能.在完成 ETPM 的搭建之后,我们将其应用于可信 PDA 这一嵌入式系统中进行测试,取得了较好的效果.

可信 PDA 中,启动引导程序和操作系统的二进制可执行代码都存在外部存储器(NandFlash)中.因此,在可信 PDA 的启动过程中,要解决以下问题:

1) 上电后,TPM 必须先进行完整性检验,此时 PDA 还不能启动,在 TPM 校验通过后,PDA 开始启动;

2) TPM 要读取外部存储器的数据进行完整性校验,这样就存在 2 个设备需要访问外部存储器:ARM 和 TPM,因此要对外部存储器的总线进行仲裁.

由于缺乏启动控制能力和总线仲裁能力,传统的 TPM 难以解决以上 2 个问题.但是 ETPM 的设计与实现,解决了这 2 个难题.

ETPM 与可信 PDA 原型系统模块关系如图 8 所示:

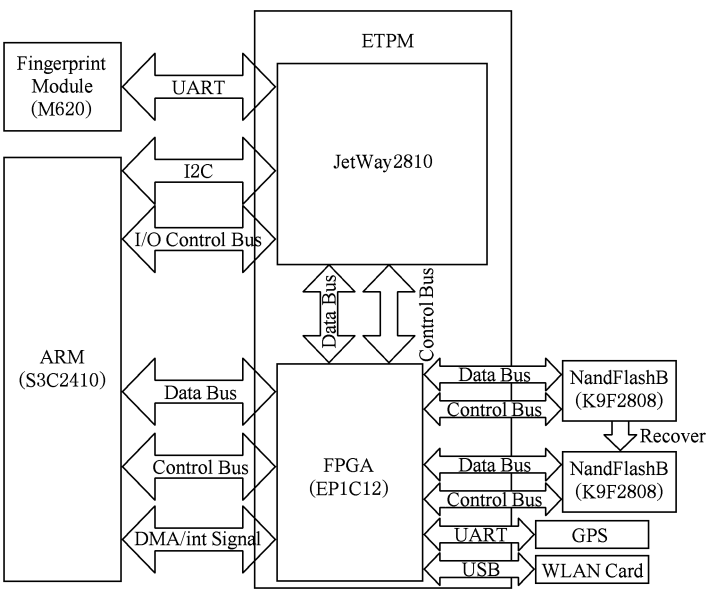


Fig. 8 ETPM and trusted PDA prototype system.

图 8 ETPM 与可信 PDA 原型系统模块图

图 8 中,JetWay2810 是瑞达公司生产的安全芯片,可以完成传统 TPM 的基本功能,在此基础上,我们将 FPGA 作为扩展模块,与 JetWay2810 以总线形式相连接,共同构成 ETPM.FPGA 在 ETPM 中充当了总线仲裁器和对称加解密引擎,并与 JetWay2810 协作,完成系统备份恢复.

两块 NandFlashA 和 NandFlashB 通过 FPGA 与 ARM 相连.其中,NandFlashA 作为系统默认存储器,NandFlashB 作为备份芯片(该芯片受到 ETPM 保护,只能读不能写),如果 ETPM 检查出 NandFlashA 中的内容被非法改动,将自动使用 NandFlashB 进行恢复.

在可信 PDA 中,平台作为从机,由 ETPM 控制计算机系统的启动过程(图 9):平台启动之前,ETPM 对引导程序、操作系统分别进行完整性测量,并将该次完整性测量结果与 ETPM 中预先存储的完整性度量值比较,判断其是否可信,只有被 ETPM 判定为可信的代码才能执行.ETPM 还支持

应用程序扩展,可对重点应用程序提供信任链扩展功能.在完整性验证过程中如果出现错误,ETPM将自动调用备份恢复模块,进行系统恢复.

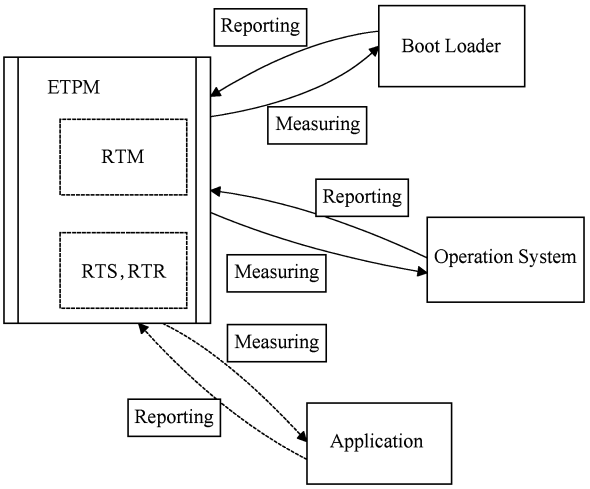


Fig. 9 ETPM trusted boot.

图 9 ETPM 可信启动

系统通过完整性验证之后,ETPM 允许 CPU 运行,可信 PDA 正常启动、工作.在此后的系统运行过程中,ETPM 仍处于监控状态,发现异常情况可以随时终止可信 PDA 系统对外部存储器设备的读写,并可控制无线网卡、GPS 等外设的使用.

在可信 PDA 的使用过程中,当需要对称加解密时,ETPM 自动调用 SMS4 引擎进行加解密.该引擎加密块大小为 512 B,处理速度近 8 MB/s.

从可信 PDA 的可信启动过程和加解密引擎的使用可以看出,ETPM 在加入总线仲裁模块和备份恢复模块之后,其控制能力有了较大提高,可以在嵌入式系统环境下很好地实现星型信任链扩展过程,减少了信任损失.同时,高速硬件对称加解密引擎加快了对称加解密速度.可见,这种设计较之传统 TPM 更加符合嵌入式环境.

4.2 实验结果分析

本实验将 ETPM 应用到具体平台中,实现了嵌入式系统的可信启动.通过实际系统的测试,证明该 ETPM 可以正确完成设计的功能.下面将从 ETPM 特点、执行效率方面对实验进行分析.

4.2.1 ETPM 特点

本设计中,ETPM 在系统启动过程中处于核心地位,它可以方便地通过总线仲裁模块实现嵌入式系统的可信启动.与传统 TPM 相比,本设计主要特点见表 1:

Table 1 Comparison of ETPM and TPM

表 1 ETPM 与 TPM 比较

Characteristics	ETPM	TPM
Start-up Control	Yes	No
Loss of Trust	Small	Large
Symmetric Cryptographic Engine	Yes	No
Reliability	High	Normal

1) 启动控制方便、灵活.ETPM 通过对总线控制模块中控制寄存器的操作,可以灵活控制可信嵌入式平台的启动.ETPM 控制下的嵌入式系统可信启动已申请国家发明专利并获得授权(专利号:ZL200710053330.7).

2) 信任损失小.本文设计的 ETPM 可以在可信嵌入式系统中实现星型信任启动机制.该启动机制的建立,能有效减少信任传递过程中的信任损失.

3) 硬件对称加解密引擎.本设计将对称加解密引擎引入 ETPM,使其具备独立对称加解密能力.

4) 可靠性高. ETPM 具备备份恢复能力,使嵌入式平台核心程序在遇到非法改动时能进行自动恢复,有效提高了 ETPM 所在嵌入式系统运行的可靠性.

4.2.2 执行效率分析

本实验中,ETPM 通过控制模块来控制可信嵌入式系统的启动流程.由于在启动过程中,需要对底层配置进行完整性校验,这一校验过程的时间要求不能太长,如果过长,虽然能完成校验功能,但是也失去了应用的意义.

在嵌入式系统 CPU 启动之前,需要对嵌入式系统上的引导程序和操作系统内核进行验证.需要验证的程序大小大约为 1 MB(67 KB 的引导程序和 824 KB 的操作系统内核).通过实际验证,本实验系统整个启动流程所花费的时间小于 0.1 s,验证的速度将近 10 MB/s,对于嵌入式应用来说,这一速度完全足够.

ETPM 内部硬件实现了 SMS4 对称密码加解密引擎,经测试,该引擎的执行速度达到 8 MB/s.为了与软件加解密进行对比,本次实验还在可信 PDA 中软件实现了 SMS4 算法,经测试,软件版本速度为 77.81 KB/s.可见,ETPM 内部的硬件对称加解密引擎大大提高了加解密速度.

由效率分析可知,ETPM 执行效率高,对嵌入式系统的启动和使用基本没有影响,证明了 ETPM

设计的高效性.同时,通过可信 PDA 的实际使用,证明了该设计的实用性.

5 总 结

本文分析了嵌入式环境对 TPM 的特殊需求,设计了一种嵌入式环境下的可信平台模块(ETPM),该 TPM 符合 TCG 规范,并且更加符合嵌入式系统特性.ETPM 的设计,增强了 TPM 对嵌入式系统的控制能力,有效提高了 ETPM 所在可信平台运行的可靠性,加快了嵌入式系统的对称加解密速度,并且可以在嵌入式系统中实现星型信任启动机制.文章最后,通过实例分析,证明了 ETPM 的设计是实用、高效、可靠、安全的.

本研究的重点目前主要侧重于可信平台模块在嵌入式系统环境下的功能性设计,对可信平台模块的硬件安全防范措施尚缺乏考虑,下一阶段我们将在这方面继续展开深入的研究.

参 考 文 献

[1] Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. Survey of information security [J]. Science in China: Information Sciences, 2007, 37(1): 129-150 (in Chinese)
(沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学: 信息科学, 2007, 37 (1): 129-150)

[2] TCG. TCG Mobile Trusted Module Specification Version 1.0 [EB/OL]. Oregon: TCG, 2007 [2010-03-10]. http://www.trustedcomputinggroup.org/specs/mobilephone/tcg2mobile2tusted2module21.0.pdf

[3] TCG. TCG Mobile Reference Architecture Version 1.0 [EB/OL]. Oregon: TCG, 2007 [2010-03-10]. http://bilephone/tcg2mobile2reference2architecture21.0.pdf

[4] Zheng Yu, He Dake, He Mingxing. Trusted computing based user authentication for mobile equipment [J]. Chinese Journal of Computers, 2006, 29(8): 1255-1264 (in Chinese)
(郑宇, 何大可, 何明星. 基于可信计算的移动终端用户认证方案. 计算机学报, 2006, 29(8): 1255-1264)

[5] Chen Shuyi, Wen Yingyou, Zhao Hong. Conceptual design of trusted mobile platform [J]. Journal of Northeastern University: Natural Science, 2008, 129(8): 1096-1099 (in Chinese)
(陈书义, 闻英友, 赵宏. 基于可信计算的移动平台设计方案. 东北大学学报: 自然科学版, 2008, 129(8): 1096-1099)

[6] Wang Yu, Wang Zhenyu, Yao Lining. Design and implementation of TPM extension and trusted bootstrap on embedded platform [J]. Computer Engineering and Design, 2009, 30(9): 2089-2091 (in Chinese)
(王禹, 王震宇, 姚立宁. 嵌入式平台 TPM 扩展及可信引导设计与实现. 计算机工程与设计, 2009, 30(9): 2089-2091)

[7] Sun Yong, Chen Wei, Yang Yixian. Trust computing of embedded systems [J]. China Information Security, 2006, (9): 50-52 (in Chinese)
(孙勇, 陈伟, 杨义先. 嵌入式系统的可信计算[J]. 信息安全与通信保密, 2006, (9): 50-52)

[8] Shen Changxiang, Zhang Huanguo, Wang Huaimin, et al. Research on trusted computing and its development [J]. Science in China: Information Science, 2010, 40(2): 139-166 (in Chinese)
(沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2): 139-166)

[9] TCG. TPM Main Part 2 TPM Structures, Specification Version 1.2 [EB/OL]. [2010-03-10]. http://www.trustedcomputinggroup.org/, 2005

[10] Camenisch J. Better privacy for trusted computing platforms [G] //LNCS 3193: Proc of ESORICS 2004. Berlin: Springer, 2004: 73-88

[11] Eisenbarth T, Güneysu T, Paar C. Reconfigurable trusted computing in hardware [C] //Proc of STC'07. New York: ACM, 2007: 15-20

[12] Li Fenghua, Wang Wei, Ma Jianfeng, et al. Enhanced architecture of TPM [C] //Proc of ICYCS'08. Washington DC: IEEE, 2008: 1532-1537

[13] Zheng Yan, Cofta P. A mechanism for trust sustainability among trusted computing platforms [G] //LNCS 3184: Proc of TrustBus 2004. Berlin: Springer, 2004: 11-19

[14] TCG Web Site [OL]. [2010-03-10]. http://www.trustedcomputinggroup.org

[15] TCG 规范列表 [OL]. [2010-03-10]. http://www.trustedcomputinggroup.org/specs/

[16] Zhao Bo, Zhang Huanguo, Li Jing, et al. The system architecture and security structure of trusted PDA [J]. Chinese Journal of Computers, 2010, 33(1): 82-92 (in Chinese)
(赵波, 张焕国, 李晶, 等. 可信 PDA 计算平台系统结构与安全机制[J]. 计算机学报, 2010, 33(1): 82-92)

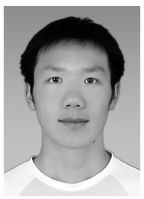
[17] Zhang Huanguo, Luo Jie, Jingang, et al. Development of trusted computing research [J]. Journal of Wuhan University: Natural Science Edition, 2006, 52(5): 513-518 (in Chinese)
(张焕国, 罗婕, 金刚, 等. 可信计算研究进展[J]. 武汉大学学报: 理学版, 2006, 52(5): 513-518)

[18] Shen Changxiang, Zhang Huanguo, Feng Dengguo, et al. Survey of information security [J]. Science in China: Series F, 2007, 50(3): 273-298

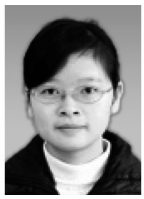
[19] Hu Zhongting, Han Zhen. Research and implementation of operating system secure trusted chain [J]. China Information Security, 2007, (2): 47-49 (in Chinese)

(胡中庭, 韩臻. 操作系统安全可信链的研究与实现[J]. 信息安全与通信保密, 2007, (2): 47-49)

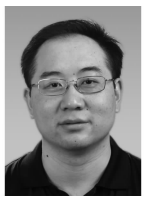
Zhang Huanguo, born in 1945. Professor and PhD supervisor. Senior member of China Computer Federation. His main research interests include information security, cryptography, and trusted computing.



Li Jing, born in 1984. PhD candidate. His main research interests focus on trusted computing.



Pan Danling, born in 1986. Master candidate. Her main research interests focus on trusted computing.



Zhao Bo, born in 1972. PhD and professor. Senior member of China Computer Federation. His main research interests include trusted computing.