可信 PDA 计算平台系统结构与安全机制

赵 波[1),2)] 张焕国[1),2)] 李 晶[1),2)] 陈 璐[1),2)] 文 松[1),2)]

[1)](武汉大学计算机学院 武汉 430079)

[2)](空天信息安全与可信计算教育部重点实验室 武汉 430079)

摘 要 PDA 作为一种手持设备,面临着众多的安全问题.文中利用可信计算思想构造了可信 PDA 的体系结构与安全机制.首先提出了一种带数据恢复功能的星型信任结构,其在安全性、效率及可靠性等方面较 TCG 的链式信任结构都有很大提升.在此基础上,进一步使用总线仲裁等技术构造了可信 PDA 的体系结构模型.文中还提出并实现了针对可信 PDA 嵌入式操作系统的安全增强、基于可信 PDA 平台的可信网络连接(TNC)以及 SD 卡全卡加密等新的安全技术与方法.在此基础上,给出一种可信 PDA 的原型系统.经过实验验证,这款可信 PDA 在各方面都达到了可信计算平台的技术要求.

关键词 可信计算;可信计算平台;可信 PDA;星型信任结构

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00082

The System Architecture and Security Structure of Trusted PDA

ZHAO Bo[1),2)] ZHANG Huan-Guo[1),2)] LI Jing[1),2)] CHEN Lu[1),2)] WEN Song[1),2)]

[1)](*School of Computer, Wuhan University, Wuhan* 430079)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan* 430079)

Abstract PDA as a handheld device, faced with a number of security issues. This paper describes the Trusted PDA architecture and security mechanism by using the method of Trusted Computing. Firstly this paper proposes a "star-style" chain of trusted structure with data recovery functions, and it owns more safety, efficiency and reliability than the TCG trust structure. On this basis, the further use of technologies such as bus arbitration system constructs a trusted structural model of PDA. The paper also proposes and implements a security enhanced embedded operating system for the trusted PDA. Based on trusted platform, Trusted Network Connect (TNC), as well as SD cards full-disk encryption and other new security technologies and methods can be solved. On this basis, the authors have developed a trusted PDA-prototype system, and this PDA has reached all aspects of the technical requirements of the Trusted Computing Platform.

Keywords trusted computing, trusted computing platform, trusted PDA, star-style chain of trusted structure

1 引 言

长期以来,很多人认为 PDA 系统的软件是固化在硬件芯片里面的,不存在被攻击的可能性,因此对于 PDA 系统的安全问题,业界并没有给予重视和研究.然而,随着 PDA 的技术发展与广泛应用,PDA 也面临着巨大的安全威胁:首先,PDA 是一种

收稿日期:2009-07-24;最终修改稿收到日期:2009-11-03.本课题得到国家自然科学基金(60673071,60970115)、国家"八六三"高技术研究发展计划项目基金(2006AA01Z442,2007AA01Z411)资助.**赵 波**,男,1972 年生,博士,副教授,主要研究方向为可信计算.E-mail: zhaobo@whu.edu.cn.**张焕国**,男,1945 年生,教授,主要研究领域为信息安全、可信计算等.**李 晶**,男,1984 年生,博士研究生,主要研究方向为可信计算.**陈 璐**,女,1979 年生,博士研究生,主要研究方向为可信计算.**文 松**,男,1975 年生,博士研究生,主要研究方向为可信计算.

手持移动设备，容易丢失，由此可能被冒用，造成信息泄露；其次，由于存储器技术的发展，PDA 的存储器越来越多地采用可编程 FLASH 器件. 因此病毒等恶意代码完全可以攻击 PDA 系统；再其次，PDA 的主要通信方式为无线通信，因此会产生电磁再次辐射，极易造成通信信息的泄露.

目前，对 PDA 设备及嵌入式系统安全增强的方法，大部分还是采用诸如 SD 卡加密等对敏感数据进行保护的传统安全技术. 这种安全保护并没有从体系结构和操作系统等软硬件底层提供根本性的安全保障.

可信计算技术是近年来出现的一种新的信息系统安全技术，目前已在世界范围形成了热潮. 它是提高计算机系统安全性的行之有效的新技术，因此也是解决 PDA 安全问题的有效途径.

国内外众多研究机构、学者已经对该领域开展了许多研究工作，并取得了一定的成果：可信计算组织 TCG 已经提出了用于解决移动平台的安全规范①②和设想，但是尚未有任何具体的实现理论和技术的说明；Intel、IBM、NTT 等公司提出了可信移动平台（Trusted Mobile Platform，TMP）项目，以 TCG 的可信平台模块（Trusted Platform Module，TPM）为基础，提出了可信移动平台的软件、硬件体系结构和协议规范③④⑤⑥，但同样缺乏具体的实现方案；国内的其他学者[1-4]也提出了利用该 TPM 模块与嵌入式 CPU 进行通信，以改善嵌入式系统安全水平的方法，这些平台构建方案都是基于 TPM 模块，现有 TPM 模块是针对 PC 终端设计的，并不能满足移动平台特有的属性和应用需求，也没有解决 TPM 和嵌入式 CPU 的双 CPU 结构对系统的控制等问题.

目前，基于 TCG 的规范标准，已经有了比较成熟的可信 PC 产品，TCG 对可信 PC[5]的链式信任关系的定义和实现值得研究可信嵌入式平台借鉴. 本文描述的可信 PDA 在理论上提出了适合嵌入式系统的带数据恢复功能的星型信任结构，并使用总线仲裁等新技术来管理 TPM 和嵌入式 CPU，解决了安全控制和系统应用之间的矛盾，提高了嵌入式系统的可信性和工作效率. 可信 PDA 还支持基于硬件的存储设备加密、基于硬件的外部设备安全管理等功能、操作系统安全增强和可信网络连接（TNC），基本实现了可信计算对嵌入式系统安全的期望.

2　可信 PDA 的体系结构

可信 PDA 除提供一般 PDA 的功能之外，更重要的是能为用户提供可信安全保障. 可信 PDA 采用可信计算机制，利用可信平台模块（TPM）和信任链技术对系统安全性进行了增强，提高了 PDA 的安全性.

可信 PDA 由 S3c2410x ARM CPU、JetWay2810 安全芯片⑦、FPGA、指纹识别模块、GPS、WLAN 等控制芯片构成，并有 TFT 触摸屏、USB 等外部输入输出设备，采用包含图形界面的嵌入式 Linux 作为操作系统，其基本结构如图 1 所示. 除了保持传统 PDA 的特点之外，还根据可信≈可靠＋安全的学术思想[6-7]，从理论上完成了星型信任结构的设计，并从技术上实现了如下的安全特点：

（1）具有数据恢复功能的星型信任结构. 信任链是保证计算机设备可信性的一个基本手段，可信 PDA 针对嵌入式系统的自身特点和可信 PC 链式信任结构的不足之处，设计了全新的星型信任结构，这种信任结构可以降低信任传递时的损耗，提高信任传递的效率、保护可信测量根 CTRM 的物理安全等. 同时，信任结构还带有数据恢复功能，启动时如果发现软件部分不完整（包括人为的破坏和病毒的传染），则自动启动恢复功能，以备份软件覆盖受损内容，确保平台软件的完整性和可靠性.

（2）包含总线仲裁模块的 ETPM（Embedded System-TPM）新结构. 以 JetWay2810 安全芯片为 TPM 核心芯片，FPGA 以总线形式与 JetWay2810 相连，构成了包括总线仲裁和对称密码算法模块的

① TCG. TCG mobile trusted module specification version 1.0 [EB/OL]. Oregon: TCG, 2007 [2007209201]. https://www.trustedcomputinggroup.org/specs/mobilephone/tcg2-mobile2trusted2module21.0.pdf

② TCG. TCG mobile reference architecture version 1.0 [EB/OL]. Oregon: TCG, 2007 [2007209201]. https://www.trustedcomputinggroup.org/specs/mobilephone/tcg2mobile2-reference2architecture21.0.pdf

③ TMP. Trusted mobile platform hardware architecturedescription [EB/OL]. [2007206205]. http://www.trustedmobile.org/TMP-HWAD-rev1-00.pdf

④ TMP. Trusted mobile platform software architecturedescription [EB/OL]. [2007206205]. http://www.trustedmobile.org/TMP-SWAD-rev1-00.pdf

⑤ TMP. Trusted mobile platform protocol specificationdocument [EB/OL]. [2007206205]. http://www.trustedmobile.org/TMP-Protocol-rev1-00.pdf

⑥ OMTP. Open mobile terminal platform group [EB/OL]. London: OMTP, 2007 [2007209201]. http://www.omtp.org/wgs-recommendations.html#trusted

⑦ Jetway Information Security Industry Corporation. J2810 security chip [EB/OL]. 2008-04-28. http://jetsec.com.cn/third/3cp/cp-ESM.htm

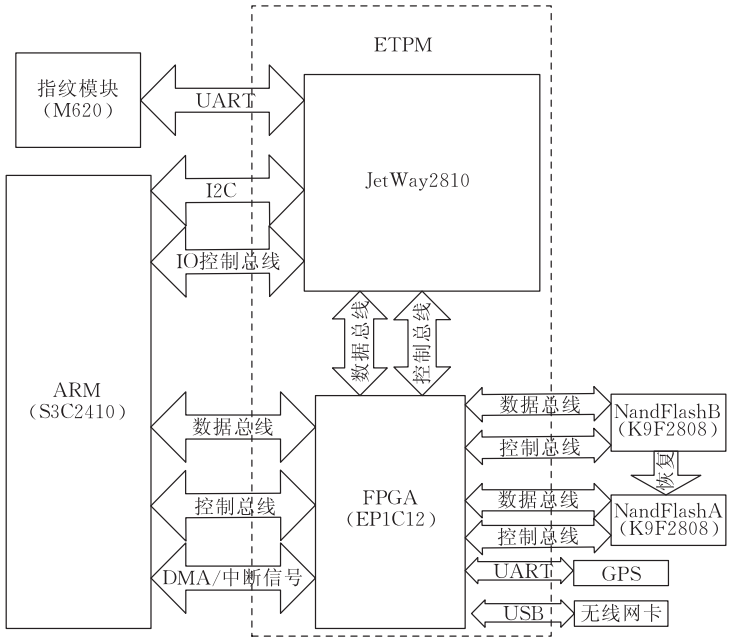


图 1 可信 PDA 体系结构框图

完整 ETPM(图 1 虚线部分),这是对 TCG 规范的一个改进.可信 PDA 上电伊始就以 TPM 为主控设备,用 TPM① 控制指纹模块对用户身份加以识别,之后对所有启动部分实施完整性度量,只有经完整性度量确认环境安全之后,才允许 ARM 平台启动.相对于目前可信 PC 的实现方案,本方法更能确保 TPM 的主控地位,提高安全性.JetWay2810 芯片还通过 FPGA 对部分外设通信信道的硬件通断进行物理层控制,如 USB 设备(包括无线网卡和 GPS).这样就做到了既安全又可控,符合我国政府的信息安全政策.

(3)操作系统安全增强.在嵌入式操作系统上实现了包括加密文件系统、重要存储区域的隔离保护、日志系统、强制访问控制等安全功能,提供全面的操作系统安全保障,为上层应用软件的安全提供了基础[8].用户身份使用指纹进行识别,并结合本机硬件特征形成各类密钥,密钥存储于 ETPM 中,并受其物理级别的保护.NandFlash 存储器中的信息,以密文形式存储,并结合硬件密码算法模块对 SD 卡实现全卡加密,被加密过的 SD 卡只能在本机使用,在其它设备上无法读取其内容,从而实现了软件和数据的防复制功能,可以防止可信 PDA 丢失后的冒用.

(4)可信网络连接.可信网络连接(TNC)是可信计算向网络领域扩展的一种重要技术.它将可信计算机制引入网络,把信任链从终端平台扩展到网络,使得网络成为一种可信的计算环境.在可信 PDA 中我们设计并实现了基于远程证明的可信网络连接(TNC)②,即在使用网络功能之前,对要接入网络的设备进行完整性验证③,以保证网络环境下应用的安全④⑤[9].

除此之外,可信 PDA 还配备了 100M 速率网卡,提供图形化的操作接口,实现了资源管理器、音频等实用功能,方便一般用户的日常工作与使用.

3 星型的信任结构

对于不同的实体,可以使用不同的组织方式来表示它们之间的相互信任关系,这种组织方式即为信任结构.对于各个实体,最直接的组织方式既为两两之间都有直接的信任关系.如图 2 所示[10].

这种相互信任结构可以非常方便地表示出各个

① Infineon. Trusted platform module [EB/OL]. 2008-04-28. http://www.infineon.com/cms/en/product/channel.html?channel=ff80808112ab681d0112ab6921ae011f

② TNC Web Site. https://www.trustedcomputinggroup.org/network/

③ TCG Specification Trusted Network Connect—TNC Architecture for Interoperability Revision 1.1[EB/OL]. Trusted Computing Group, 2006.5. http://www.trustedcomputinggroup.org

④ TCG Specification Trusted Network Connect — TNC IF-PEP: Protocol Binding for Radius Revision 0.7[EB/OL]. 2007.5. https://www.trustedcomputinggroup.org

⑤ TCG Specification Trusted Network Connect — TNC IF-TNCCS: TLV Binding Revision 10 [EB/OL]. 2008.1. https://www.trustedcomputinggroup.org

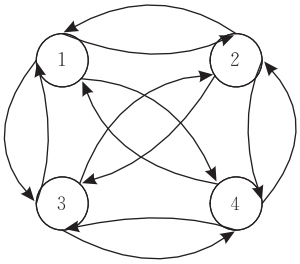


图 2　相互信任结构图

实体之间的相互信任关系，但是，这种结构需要维护的关系表很多，如果实体数量较多，实现将非常困难.

TCG 提出了一种链式的信任结构来实现实体的信任关系，与相互信任结构相比，该结构更易于实现. 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[11].

TCG 的链式信任结构存在着很多的不足之处：(1) 可信测量根 CRTM 置于 TPM 之外，不受 TPM 的物理保护，容易受到恶意攻击破坏；(2) 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某个部件，或者软件的版本升级，都必须重新计算所有的信任值，增加了维护和管理的难度；(3) 根据信任理论，信任值在传递过程中会有损耗，传递的路径越长，则损耗越大[7]. 由于链式信任结构的信任传递路径长，所以容易产生信任的损耗.

3.1　星型信任结构

基于 Dempster-Shafer 原理的计算信任值的两条原则如下[12]：

(1) 信任衰减原则

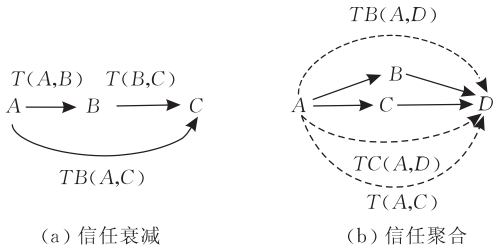
如果节点 A 对节点 B 的信任值为 $T(A,B)$，节点 B 对节点 C 的信任值为 $T(B,C)$，$TB(A,C)$ 表示经由 B 点传递的 A，C 之间的信任关系. 由传递性可以推断出 A 和 C 之间的信任关系.

定理 1.　$TB(A,C)=T(A,B)\oplus T(B,C)$.

这里符号$\oplus$表示提取两者之间信任最小值的概念，因此有 $TB(A,C)\leq\min(T(A,B),T(B,C))$.

(2) 信任聚合原则

节点 A 到节点 D 存在两条独立的路径，这两条路径分别给出它们的信任值 $TB(A,D)$ 和 $TC(A,D)$. $TB(A,D)$ 表示经由 B 点传递的 A，D 之间的信任关系，$TC(A,D)$ 表示经由 C 点传递的 A，D 之间的信任关系. 由此可以判断出 A 和 D 之间的信任关系.



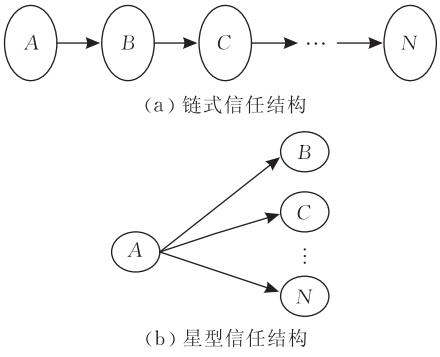
(a) 信任衰减　　(b) 信任聚合

图 3　信任基本规则

定理 2.　$T(A,D)=TB(A,D)\ominus TC(A,D)$.

这里符号$\ominus$表示提取两者之间信任最大值的概念，因此有 $T(A,D)\leq\max(TB(A,D),TC(A,D))$.

图 4 分别图示了链式信任结构和星型信任结构.



(a) 链式信任结构

(b) 星型信任结构

图 4　链式和星型信任结构

在图 4 中，依照以上两条原则递推：

由链式结构，信任链经过节点：$A\rightarrow B\rightarrow C\rightarrow D\rightarrow\cdots\rightarrow L\rightarrow M\rightarrow N$，则链式信任结构的各级信任值有 $T(A,C)=\min(T(A,B),T(B,C))$，$T(A,C)$ 表示经过 B 点的 A、C 之间的信任关系，以此类推，有 $T(B,D)=\min(T(B,C),T(C,D))$，…，其最终信任值 $Tline$ 不会大于 $\min(T(A,B),T(B,C),\cdots,T(L,M),T(M,N))$，并且，从节点 A 到节点 N 的路径上任何一个信任关系的破坏，都会完全破坏整个信任链.

结论 1.　如果依照星型信任结构，节点 A 与节点 N 之间有多条直接路径：$T_1(A,N)$，$T_2(A,N)$，$T_3(A,N)$，…，$T_n(A,N)$；则最终信任值 $Tstar$ 不会小于 $\max(T_1(A,N),T_2(A,N),T_3(A,N),\cdots,T_n(A,N))$，即总有 $Tstar\geq Tline$（$Tstar$ 在最坏情况下等于 $Tline$ 在最好情况下的值）；而且星型信任关系结构较之前者健壮[13].

结论 2.　在星型信任结构中，节点 A 一般作为信任根出现，由它进行对其它节点的度量工作，其作用相当于 TCG 定义的 TPM，然而，其具体的结构与 TPM 略有不同，星型信任结构的 TPM 将包含可信

度量根 CRTM，这样可以最大限度地保证 CRTM 在物理上是安全的.

结论 3. 星型信任结构的信任值计算是根节点与每一个测量节点之间的独立计算结果，互相之间不会产生影响，因此添加和删除组件以及软件版本升级，只需要根节点对该节点单独重新进行计算即可，不会影响到整个信任链.

将链式信任结构和星型信任结构进行比较可以看出，星型信任结构优于链式信任结构.

星型信任结构也有不足之处：在星型结构中，由于根节点处于中心位置，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，根节点的计算压力较大，可能造成平台工作效率的损失. 但是，PDA 系统有自己的特点，其 TPM 与 ARM CPU 的计算能力相当，因此 TPM 的工作不会带来系统整体性能明显的改变. 可信 PDA 原型系统的实际运行情况也证明了这一点. 所以，可信 PDA 使用星型信任结构是可行的，它保证了系统的信任度优于可信 PC 的链式信任结构.

可信 PDA 的星型信任结构以 TPM 为可信根，作为整个嵌入式平台的可信测量和控制器，嵌入式平台作为从设备受 TPM 的管理和控制；TPM 内部采用物理方式集成了可信度量根、可信存储根和可信报告根，对自身以及连接电路有良好的物理保护；TPM 启动后，只有身份信息和存储器内容的完整性验证完成之后，可信的代码才能在嵌入式平台上执行. 星型信任结构如图 5 所示. 星型信任结构和可信启动的概念，已经获得国家专利授权（专利号 ZL200710053331.1；ZL200710053330.7）.

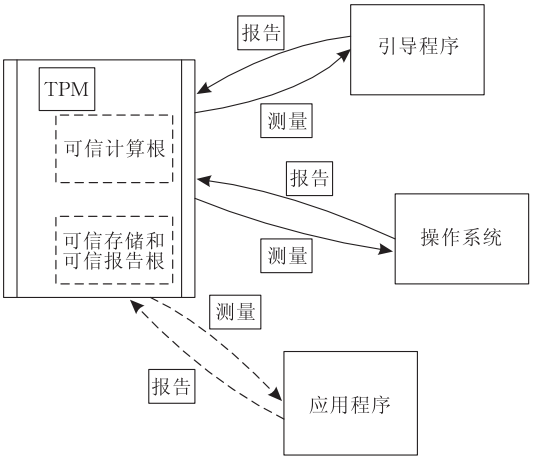


图 5 星型信任链传递过程

3.2 总线仲裁

为了实现系统启动前的星型信任结构的完整性校验，TPM 要将 NandFlash 中的 BootLoader，Linux kernel 等内容读入进行校验[14]，这就涉及到两个问题：(1) 启动顺序，在上电后，TPM 要先进行完整性检验，此时 ARM 还不能启动，在 TPM 校验通过后，ARM 开始启动；(2) S3C2410 ARM CPU 和 TPM 都需要读取 NandFlash 的值，因此需要对 Flash 读取的总线进行仲裁. 总线仲裁的体系结构设计框图如图 6 所示.

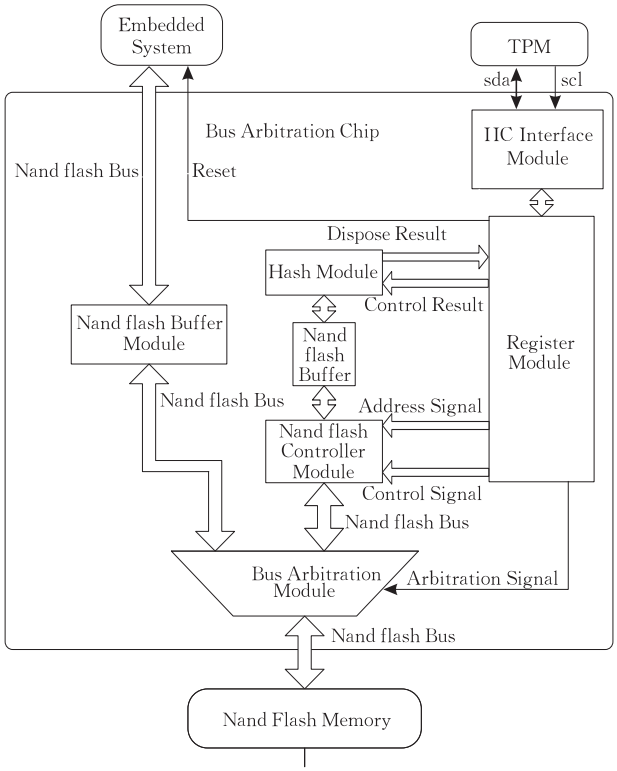


图 6 总线仲裁模块

在图 6 中，使用 FPGA 实现 S3C2410 和 TPM 对 NandFlash 的分时操作，TPM 为控制核心，由它来控制可信 PDA 的启动流程，可以根据度量情况随时将 S3C2410 关断和启动. 这种方法解决了可信 PC 中可信根度量和 BIOS 同时工作的尴尬局面，真正使 TPM 处于主控地位.

总线仲裁的实现还可以带来如下的好处：

(1) TPM 控制方便，灵活. TPM 通过对总线控制器中的控制寄存器的修改，可以完全使用程序来灵活控制 S3C2410 的启动，TPM 也可以使用程序来控制读取 NandFlash 的信息量.

(2) 扩展方便. 本模块设计了 TPM 对 S3C2410 的开启与关断，若想实现其它安全控制，如关闭某个外设，只需要对体系结构做些许修改[6,15]；此外，还可以非常容易地扩展实现 TPM 对 NandFlash 的读

写保护.从物理上保护存储设备中内容的完整性和安全性.

可信 PC 没有考虑总线仲裁问题,采用了 TPM 和 CPU 同时启动的可信根扩展的方法[16].这种方法是对现有 PC 产品的一种妥协,使得对 CRTM 的保护和对 BIOS 的度量都难于实现.这是目前可信 PC 的一个缺陷.

3.3　具有数据恢复功能的信任结构

可信 PDA 仅仅具有安全功能是不够的,根据可信≈可靠＋安全的学术思想[7](https://www.trustedcomputinggroup.org/network/),可信的产品也应该有较好的可靠性.因此,TPM 在启动时若检测到可信 PDA 的 OS、Bootloader 等已经受到了攻击并被篡改时,除了阻止 PDA 的进一步运行之外,需要提供一种机制以使得 PDA 能够恢复到其正常的状态,保证 PDA 的正常工作不受干扰.

可信 PDA 的备份恢复机制需要对 TCG 规范中的 TPM 结构进行扩展,在 TPM 内部添加一个受物理保护的系统备份存储器,保存计算机系统引导程序和操作系统等希望被保护的内容代码.TPM 在系统启动之前对 PDA 引导程序代码及操作系统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,TPM 将使用总线仲裁机制获取总线控制权,从受保护的备份存储器中读取相应的备份代码,并将其写入 PDA 外部工作用存储器,再次进行完整性校验,若通过校验,表明系统恢复成功,TPM 将交出总线控制权,允许 PDA 设备系统启动.

与现有的技术相比,该方式有如下优点:由 TPM 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.TPM 拥有可信 PDA 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.图 7为基于 TPM 控制的备份恢复体系结构.经过原型系统的实际测试,完成一次备份恢复的时间少于 1s(恢复内容小于 32MB),可以满足实际使用的要求.从而大大提高了可信 PDA 的可靠性和可用性.

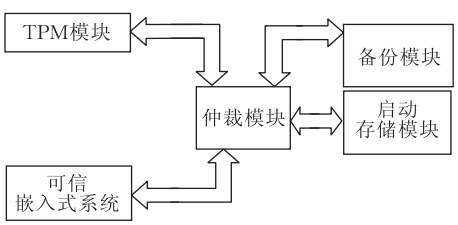


图 7　备份恢复

3.4　新型的 TPM 结构

可信 PDA 是自主研发的可信产品,目前国内尚无适合星型信任结构的 TPM 成品.由前文所述,可信 PDA 的 TPM 包含的功能比常规的 TPM 芯片多,因此,在图 1 中,以 JetWay2810 安全芯片和 FPGA 设备构成了一种新的 TPM 模块结构.

3.4.1　JetWay2810 芯片

JetWay2810 的安全芯片是一款通过国家认证的可信计算平台模块芯片.它是与 AMD186 兼容的 16 位微控制器芯片,采用经 SOSCA(Secure Open Smart Card Architecture)指令集增强的 X86 处理器内核,集成大容量存储器,多体制密码引擎,USB,ISO 7816/4 等多种外围控制器.该芯片具有基本的密码计算和 PCR 数据存储功能,经过添加 COS,JetWay2810 可以完成 TCG 规定的 TPM 的基本功能,并提供 TSS 的底层接口.

3.4.2　TPM 与 TCM

TPM 是可信计算平台的一个重要的组成部件,根据 TCG 的定义,TPM 必须由硬件来实现,但是 TCG 仅仅在理论上定义出了 TPM 应该完成的功能,对其如何实现,性能指标要求,并没有统一的实现规定,作为一个标准的 TPM,应包含执行引擎、存储器、I/O、RSA 密码引擎、随机数产生器等部件,以完成加密、签名、认证、密钥产生等安全功能.但是,TCG 的 TPM 定义中并不包含对称密码算法引擎.一般 TCG 建议利用其他的方式实现,这就带来一定的安全和性能隐患.

我国的 TCM(Trusted Cryptography Module,可信密码模块)标准[16],是由国家密码管理局主持国内一些 IT 企业推出的.TCM 与 TPM 最大的不同在于,其内部的核心密码算法为我国自主知识产权的算法标准,特别是集成了我国的对称密码算法(SMS4).这样,TCM 就避免了 TPM 中没有对称密码算法的缺陷.

3.4.3　ETPM(Embedded System TPM)

可信 PDA 由于使用了前文描述的星型信任结构,因此 ETPM 的体系结构与 TPM 和 TCM 不同,其基本结构如图 8 所示:公钥算法采用了 RSA 的 2048 位(也可使用 ECC),对称密码算法采用了 SMS4,另外还有完成正常启动顺序的总线仲裁、备份恢复模块.上述几种模块,JetWay2810 没有提供,故而采用 FPGA 硬件实现.ETPM 构成了可信 PDA 的核心根模块,可以很好地实现星型信任结构

所描述的功能，如图 1 和图 5 所示，形成了一种支持嵌入式系统的可信计算体系结构模块.

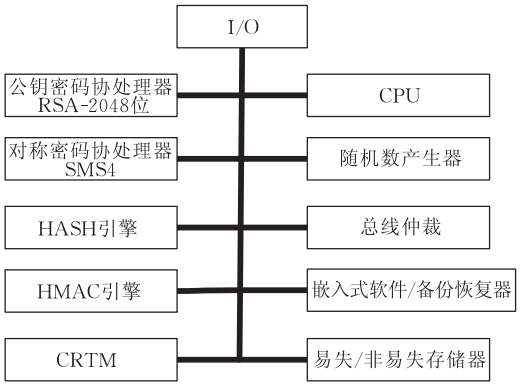


图 8 ETPM 的结构

4 存储介质和操作系统安全

对于用户而言，可信 PDA 最重要的功能之一就是要保证数据信息的安全，需要达到如下的安全效果：

(1) 实现可信 PDA 的存储介质 NandFlash 上重要数据区域的写操作保护，提供开机启动时的完整性校验支持.

(2) 保证移动设备数据存储的机密性，解决未经授权的访问和因便携式设备的失窃引发的泄密等问题.

(3) 细化文件的访问粒度，限制超级用户的权限. 即使是授权用户在访问资源时，行为必须符合安全策略，操作才能执行，否则将拒绝. 防止超级用户滥用权限.

(4) 系统的安全增强模块有可以信赖的可信计算基.

可信 PDA 应实现对用户透明的安全存储保护模式，授权用户可以像使用普通文件系统一样完成安全功能操作. 由于嵌入式操作系统资源有限，安全增强模块在内核层实现，加密模块利用 Linux 缓冲机制并调用硬件密码模块进行加密，并在访问控制机制中添加策略缓存，提高了系统性能(见本文第 3 页注释④)

4.1 存储介质的安全

可信 PDA 使用 SD 卡作为外部的数据存储器，用户的私密信息经常存储于此. 因此，SD 卡内的数据保护就显得尤为重要. SD 卡使用 TPM 中的硬件加密芯片实现加解密操作，在系统的性能和物理安全上都有极大的提高，其密钥存入 TPM 中，由 TPM 提供保护. SD 卡加密文件系统主要分为加密引擎和密钥管理两个主要部分[17]. 加密引擎是在内核合适的加解密位置调用硬件加密芯片利用 SMS4 完成加解密操作；密钥管理是使用 TSS 密钥安全存储接口访问 TPM 芯片中存储的密钥，从而利用其加密以及平台绑定功能来保证密钥的可信和安全性. 其体系结构如图 9 所示.

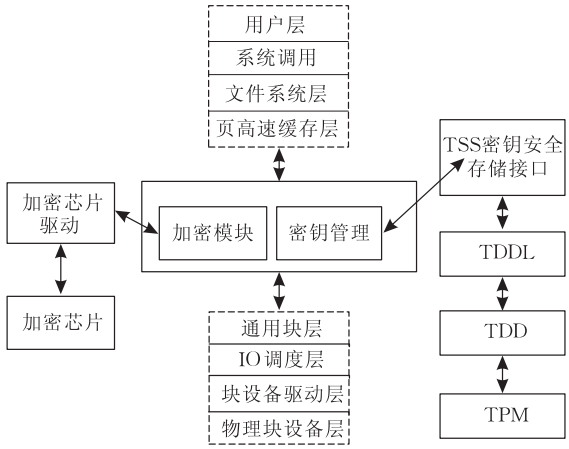


图 9 SD 卡加密文件系统体系结构

由于是在页高速缓存层和通用块层之间添加了数据加解密功能[17]，因此对于上层用户是透明的，使用户感觉不到文件的加密过程，不修改文件系统的数据结构且用户访问加密文件的过程也不变. SD 卡一旦丢失，非合法用户也无法获得其内容，因加密层在文件系统层之下，非法用户甚至连文件结构都不能读取.

4.2 数据隔离保护

嵌入式系统中，BootLoader、kernel 和根文件系统是保障系统安全的重要区域，要求用户进程不能随便改动，否则将导致系统出错甚至无法使用. 但用户存储区内的数据应可由用户任意添加、删除和修改. 因此有必要对嵌入式的存储空间进行划分，以用户是否可以自由修改为依据，可以将存储空间划分为用户数据区和系统数据区.

在操作系统启动之前，TPM 会自动校验系统数据区，校验通过后 TPM 才把控制权交给 CPU，系统运行. 至此这些区域一直由 TPM 来保护. 按照目前可信 PC 的运行模式，在操作系统开始运行之后，TPM 不会再对这些区域进行保护，恶意进程和用户的误操作可能会改写这些区域的数据，因此需要保护这些重要区域，防止被改写.

可信 PDA 中存储隔离保护设计的核心思想是在存储介质 NandFlash 上划分出一个重要分区来

进行写操作保护[18]. 因为文件系统是建立在 NandFlash 上，在读写请求被提交给 NandFlash 驱动时，NandFlash 驱动要检查写操作，如果写的位置是这些重要区域，那么 NandFlash 驱动就阻止这次写操作，并直接返回错误值给进程，以防止这些区域被篡改. NandFlash 之下是 MTD 块设备，所以确定在存储技术设备驱动中进行修改，对于 NandFlash 在执行写操作前，检查要写的地址是不是在指定的地址，如果是，则直接返回错误，否则发起写操作，从而来提供完整性保护.

可信 PDA 的 MTD 设备层次结构如图 10 所示，Flash 硬件驱动层负责在初始化时驱动 Flash 硬件；MTD 原始设备层一部分是 MTD 原始设备的通用代码[17]，另一部分是各个特定的 Flash 的数据例如分区，定义了大量的关于 MTD 的数据和操作函数；MTD 设备层是基于 MTD 原始设备，定义出 MTD 的设备号以及注册设备操作；设备节点层负责建立 MTD 字符设备节点（主设备号为 90）和 MTD 块设备节点（主设备号为 31），通过访问此设备节点即可访问 MTD 字符设备和块设备.

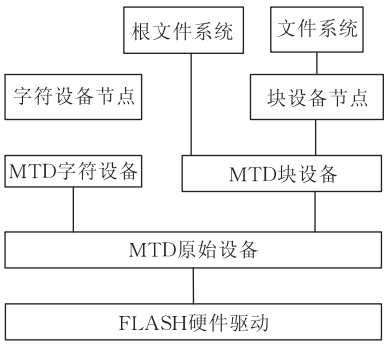


图 10　MTD 设备层次结构

4.3　操作系统内核安全增强

可信 PDA 在操作系统内核中加入钩子函数[19-20]，对标准内核进行了以安全增强为目的的修改，并以配置文件的方式实现策略逻辑. 当需要进行访问内核时，首先检查是否符合既定的安全策略，如果符合则通过本次访问，否则拒绝. 在 Linux 内核中，钩子函数被放置于 namei.c、open.c 和 readdir.c 的相关函数中. 打开文件时，钩子函数就先查找策略配置文件中的相关策略[21]，如果符合策略，则通过 read_write.c 文件中的相关函数执行读写操作，如果不符合，则直接返回错误. 图 11 所示为钩子函数的调用过程. 策略文件中保存了主体（可执行文件）、客体（数据文件）、节点号、访问权限信息，用以指明哪个主体可以哪种方式访问哪个客体[22].

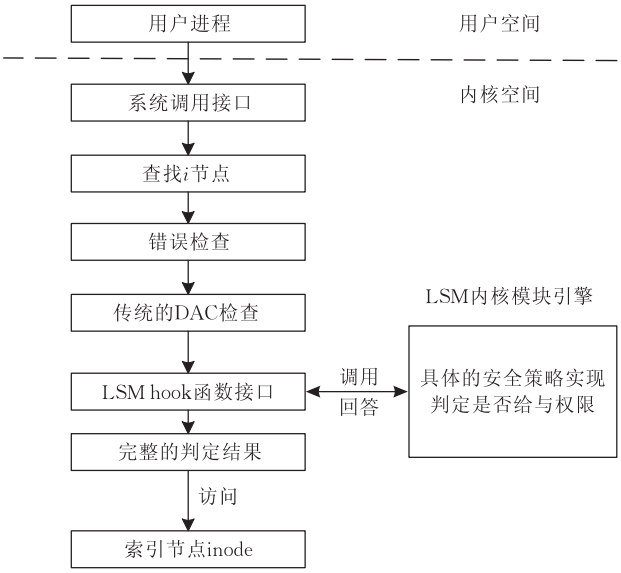


图 11　操作系统内核安全增强

该强制访问控制实现简单[23]，策略易于定制，提供策略管理工具，适于可信 PDA 的应用.

我们测试了设置为只读的文件如何实现访问控制（图 12）. 利用命令重写和追加 test_readonly 文件时，终端均显示为操作被禁止. 使用 cat 显示未经修改的文件内容，表明只读文件不可以被修改和追加.

```
[root@localhost mac]# echo "write to it"> ./test_readonly
bash: ./test_readonly: Operation not permitted
[root@localhost mac]# echo "write to it">> ./test_readonly
bash: ./test_readonly: Operation not permitted
[root@localhost mac]# cat ./test_readonly
this is a test of readonly capability for MAC.
[root@localhost mac]#
```

图 12　测试属性为只读的客体

4.4　日志系统

普通的嵌入式 Linux 并不带有日志功能[24]，为了让用户了解可信 PDA 的运行状态，进一步增强可信 PDA 的安全性[16]，并为日后的审计工作提供依据，我们为可信 PDA 增加了日志功能.

可信 PDA 在嵌入式 Linux 内核源码中编译加入了 syslog 模块，能够有效节省空间. 同时，syslog 带有日志轮转功能，能够通过对 syslog 加命令行参数来打开日志轮转的功能，不需要另外增加 logrotate 程序，以提高日志记录效率. 经过综合考虑与原型系统的实验，由于可信 PDA 目前所要记录的日志量不大，种类也不多，为实现简单起见，采用交叉编译的方法，将 syslog 编译到 busybox 中即可，不需要另外添加 logrotate 工具.

可信 PDA 上的日志系统主要记录以下事件：

(1) 内核的输出信息；

(2)应用程序的日志;

(3)系统出错信息.

通过对日志的分析,用户能够了解可信 PDA 的运行状况,及时发现安全隐患,防范于未然,并为日后的审计工作提供依据.

5 可信的网络连接

在基于远端证明的可信 PDA 无线网络接入控制方案中,PDA 与终端建立连接之前,首先对终端的身份进行认证,保证只有特定的终端才可以与 PDA 进行连接;在身份认证通过之后,对终端的平台状态进行验证;若符合要求,则允许终端与其建立连接,这样可以避免由于终端自身的安全问题而导致可信 PDA 上的数据遭到破坏. 在实现系统中,主要有 3 个实体:可信 PDA、接入终端和完整性参考服务器. 系统架构如图 13 所示.

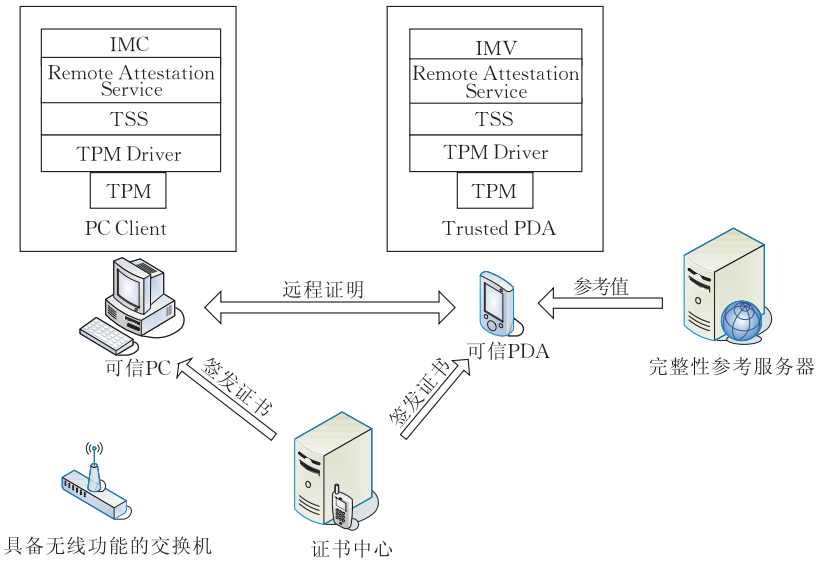


图 13 远程证明的系统结构

在该系统中,终端(即上图可信 PC)与可信 PDA 进行远程证明,完整性参考服务器具有双方平台的标准完整性参考值. 可信 PDA 通过无线网络与终端及完整性参考服务器相连接,终端及 PDA 都有 TPM 作支持. 可信 PC 上完成远程证明的功能组件主要包括自行开发的 TSS(见 TNC IF-TNCCS), Remote Attestation Service 和 IMC(Integrity Measurement Collector),负责读取平台的 PCR 及 EventLog 等信息并报告给 PDA. 可信 PDA 上的功能组件主要包括 TSS, Remote Attestation Service 和 IMV(Integrity Measurement Verifier),负责验证要求接入的平台是否可信(见 TNC IF-PEP). 证明过程如下:

(1)终端正常工作,通过有线或无线网络连入局域网;完整性参考服务器正常工作,通过有线网络连入局域网;可信 PDA 正常工作,通过无线网络连入局域网.

(2)可信 PDA 从终端获取其 TPM 中的 PCR 值和 EventLog.

(3)可信 PDA 通过 EventLog 计算 PCR,并与获取的 PCR 比较,匹配则继续,否则判断终端不可信,程序结束.

(4)可信 PDA 从完整性参考服务器获取标准 EventLog 值,并参照它验证从终端获取的 EventLog,从而判断终端的安全状态.

(5)若匹配则说明远程证明成功,终端可信,否则终端不可信.

通过以上过程,可以利用可信 PDA 对接入网络的终端进行可信验证,从而实现可信网络连接,在此基础上,可以完成可信数据传输,可信资源共享,进一步向可信网络的应用发展.

6 结 论

本文提出了一种带数据恢复功能的星型信任结构,其在安全性、效率及可靠性等方面较 TCG 的链式信任结构都有很大提升. 在此基础上,进一步使用总线仲裁等技术构造了可信 PDA 的体系结构模

型.文中还提出并实现了针对可信 PDA 嵌入式操作系统的安全增强、基于可信 PDA 平台的可信网络连接(TNC)以及 SD 卡全盘加密等新的安全技术与方法.这些理论和方法是对可信计算技术的有益发展,对 PDA 等嵌入式平台实现可信计算技术具有一定的应用价值,而且对解决目前可信 PC 的一些问题也提供了较好的思路.

可信 PDA 的研究工作是在国家"八六三"项目支持下进行的,通过理论研究和技术实践,研制出我国第一款具有自主知识产权的可信 PDA 原型系统,如图 14 所示.经过实验验证,这款可信 PDA 在各方面都达到了可信计算平台的技术要求,实现了构建可信嵌入式系统的目标.

图 14　可信 PDA 的原型系统

参　考　文　献

[1] Zheng Yu, He Da-Ke, He Ming-Xing. Trusted computing based user authentication for mobile equipment. 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)

[2] Chen Shu-Yi, Wen Ying-You, Zhao Hong. Conceptual design of trusted mobile platform. 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)

[3] Wang Yu, Wang Zhen-Yu, Yao Li-Ning. Design and implementation of TPM extension and trusted bootstrap on embedded platform. 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)

[4] Sun Yong, Chen Wei, Yang Yi-Xian. Trust computing of embedded system. 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. 信息安全与通信保密, 2006, (9): 50-52)

[5] Shen Chang-Xiang, Zhang Huang-Guo, Feng Deng-Guo et al. Survey of information security. Science in China Series E: Information Security, 2007, 37(2): 129-150

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

[7] Shen Chang-Xiang, Zhang Huan-Guo, Feng Deng-Guo, Cao Zhen-Fu, Huang Ji-Wu. Survey of information security. Science in Chian Series F, 2007, 50(3): 273-298

[8] ISO/IEC. Information technology—Open systems interconnection-Evaluation criteria for information technology. New York: Standard ISO/IEC 15408, 1999

[9] Smith B C. Procedural reflection in programming languages [Ph. D. dissertation]. MIT, 1982

[10] Liu Wan, Tan Ming, Zheng Jun. Trusted boundary extension model based on trusted chain on platform. Computer Engineering, 2008, 34(6): 176-181(in Chinese)
(刘皖,谭明,郑军. 基于平台可信链的可信边界扩展模型. 计算机工程, 2008, 34(6): 176-181)

[11] Hu Zhong-Ting, Han Zhen. Research and implementation of operating system secure trusted chain. 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. 信息安全与通信保密, 2007, (2): 47-49)

[12] Zhang Jing-Mei, Jin Yan. Studies on trust models of P2P network security. Journal of University of Jinan (Science and Technology), 2002, 16(4): 343-345(in Chinese)
(张京楣,金妍. 基于对等网络的信任模型. 济南大学学报(自然科学版), 2002, 16(4): 343-345)

[13] Arbaugh W, Farber D, Smith J. A secure and reliable bootstrap architecture//Proceedings of the IEEE Symposium on Security and Privacy, 1997: 65-71

[14] Yang Wei. The analysis of PC booting mechanism and the design of safe booting system[M. S. dissertation]. PLA Information Engineering University, Zhengzhou, 2005(in Chinese)
(杨伟. PC 机引导系统分析及安全引导系统设计[硕士学位论文]. 中国人民解放军信息工程大学, 郑州, 2005)

[15] Mao Jian, Zhou Yu-Jie. Trusted platform module countermeasures against hardware attacks. Information Technology, 2006, 30(6): 27-29, 52(in Chinese)
(毛健,周玉洁. 可信平台芯片的一种硬件攻击防范设计. 信息技术, 2006, 30(6): 27-29, 52)

[16] Chen You-Lei. Study on trusted computing model and architecture[Ph. D. dissertation]. Wuhan: Wuhan University, 2006(in Chinese)
(陈幼雷. 可信计算模型及体系结构研究[博士学位论文]. 武汉大学, 武汉, 2006)

[17] Qing Si-Han, Liu Wen-Qing. Introduction to Operating System Security. Beijing: Science Press, 2003(in Chinese)

(卿斯汉,刘文清. 操作系统安全导论. 北京:科学出版社,2003)

[18] Liu Ke-Long, Feng Deng-Guo, Shi Wen-Chang. Secure Operating System Principle and Technology. Beijing: Science Press, 2004(in Chinese)
(刘克龙,冯登国,石文昌. 安全操作系统原理与技术. 北京:科学出版社,2004)

[19] Cai Yi, Shen Chang-Xiang. The status and countermeasures of secure operation system//Proceedings of the 16th National Computer Security Academic Communication Conference. Chengdu, Sichuan, 2001: 1-5(in Chinese)
(蔡谊,沈昌祥. 安全操作系统发展现状及对策//第 16 次全国计算机安全学术交流会. 四川,成都,2001: 1-5)

[20] Yang Tao, Chen Fu-Jie, Shen Chang-Xiang. Design of a secure operating system S-UNIX. Chinese Journal of Computers, 1993, 16(6): 409-415(in Chinese)
(杨涛,陈福接,沈昌祥. 一个安全操作系统 S-UNIX 的研究与设计. 计算机学报,1993,16(6):409-415)

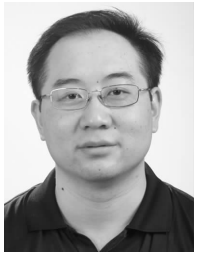
[21] Chen Zhi-Ping, Lei Hang, Yang Xia, Li Huan. Research and realization of embedded security operating system. Computer Engineering, 2007, 33(1): 83-85, 103(in Chinese)
(陈志平,雷航,杨霞,李欢. 嵌入式安全操作系统的研究和实现. 计算机工程,2007,33(1):83-85,103)

[22] Charles P Pfleeger, Shari Lawrence Pfleeger. Security in Computing. 3rd Edition. Beijing: Publishing House of Electronics Industry, 2004: 400-418(in Chinese)
(Charles P Pfleeger, Shari Lawrence Pfleeger, 李毅超等译. 信息安全原理与应用. 第 3 版. 北京:电子工业出版社,2004:400-418)

[23] Liu Hai-Feng, Qing Si-Han et al. Design and realization of Auditing in security operating system. Journal of Computer Research and Development, 2001, 38(10): 1262-1268(in Chinese)
(刘海峰,卿斯汉等. 安全操作系统审计的设计与实现. 计算机研究与发展,2001,38(10):1262-1268)

[24] Wu Xing-Yong. Research on security techniques of embedded operating system [Ph. D. dissertation]. School of Computer Science and Engineering, University of Electronics Science and Technology of China, Chengdu, 2003(in Chinese)
(吴兴勇. 嵌入式操作系统安全保障技术研究[博士学位论文]. 电子科技大学计算机学院,成都,2003)

[25] Wang Zhen-Yu, Liu Xin-Jie. Key technologies for trusted computing environment on embedded terminal. Computer Engineering, 2008, 34(22): 239-244(in Chinese)
(王震宇,刘鑫杰. 嵌入式终端可信计算环境的关健技术. 计算机工程,2008,34(22):239-244)



ZHAO Bo, born in 1972, Ph. D., associate professor. His main research interest is in trusted computing.

ZHANG Huan-Guo, born in 1945, professor, Ph. D. supervisor. His main research interests include information security, cryptography, trusted computing.

LI Jing, born in 1984, Ph. D. candidate. His main research interests focus on trusted computing.

CHEN Lu, born in 1979, Ph. D. candidate. Her main research interests focus on trusted computing.

WEN Song, born in 1975, Ph. D. candidate. His main research interests focus on trusted computing.

Background

This work is supported by the National Natural Science Foundation of China (60673071,60970115) and the National High Technology Research and Development Program (863 Program) of China (2006AA01Z442,2007AA01Z411).

With the development of PDA technology and it's wide application, PDA is facing a huge security threat. Trusted computing technology is a new emerging security technology which serves as an effective way to improve the safety and security of computer system , thus a feasible way to solve the PDA's security issues.

Currently, Trusted Computing Group (TCG) has proposed some specifications to solve mobile platform's security issues. But there is no specific instruction on how to realize it. Some companies such as Intel, IBM, NTT have proposed TMP (Trusted Mobile Platform) projects without details on how to implement them. There are some scholars also suggest improving embedded system's security status by using TPM to communicate with embedded CPU. However, these suggestions do not meet the mobile platform's specific meets since the platforms proposed are all based on TPM which was designed for PC terminal, and the control problem caused by TPM and embedded CPU's dual-CPU structure is still to be solved.

This group integrated trusted computing technology with the security of PDA, gave an in-depth discussion in theories and technologies of trusted-PDA, and developed the first domestic trusted-PDA prototype system. This prototype can provide following functions: enable users to identify themselves by fingerprint, ensure the integrity of system resource, security data storage, trusted network connect, remote attestation of platform, GPS locating and so on.