

可信计算系统及其研究现状

秦中元, 胡爱群

(东南大学无线电工程系, 南京 210096)

摘 要: 可信计算是信息安全研究的一个新阶段, 它通过在计算设备硬件平台上引入安全芯片架构, 通过其提供的安全特性来提高整个系统的安全性。该文简要介绍了可信计算的起源和发展, 重点分析了可信计算系统的体系结构和可信平台模块、可信根等关键技术, 并对目前的研究现状作了总结。

关键词: 可信计算系统; 可信平台模块; 可信根

Trusted Computing System and Its Current Research

QIN Zhongyuan, HU Aiqun

(Department of Radio Engineering, Southeast University, Nanjing 210096)

【Abstract】 Trusted computing is the new stage of information security. It brings security chip architecture in the computing hardware platform, and the whole system's security is greatly improved correspondingly. The origin and development of trusted computing are introduced, especially its architecture and the key components such as the trusted platform module, root of trust, etc. The current research has also been concluded.

【Key words】 Trusted computing system; Trusted platform module; Root of trust

1 可信计算系统的起源和发展

计算机和通信技术的迅猛发展使得信息安全的地位日益显得重要。目前的信息安全技术主要依靠强健的密码算法与密钥相结合来确保信息的机密性、完整性, 以及实体身份的惟一性和操作与过程的不可否认性。但是各种密码算法都并非绝对安全, 而且很多用户并不清楚这些密码保护机制如何设置, 更重要的是, 这些技术虽然在一定程度上可以阻挡黑客和病毒的攻击, 但是却无法防范内部人员对关键信息的泄露、窃取、篡改和破坏。

沈昌祥院士指出常规的安全手段只能是以共享信息资源为中心在外围对非法用户和越权访问进行封堵, 以达到防止外部攻击的目的; 对共享源的访问者源端不加控制; 操作系统的不安全导致应用系统的各种漏洞层出不穷; 恶意用户的手段越来越高明, 防护者只能将防火墙越砌越高、入侵检测越做越复杂、恶意代码库越做越大。从而导致误报率增多、安全投入不断增加、维护与管理更加复杂和难以实施以及信息系统的使用效率大大降低。于是近年来信息安全学界将底层的计算技术与密码技术紧密结合, 推动信息安全技术研究进入可信计算技术阶段。

1999年10月, 为了提高计算机的安全防护能力, Intel、微软、IBM、HP和Compaq共同发起成立了可信计算平台联盟(Trusted Computing Platform Alliance, TCPA), 并提出了“可信计算”(trusted computing)的概念, 其主要思路是增强现有PC终端体系结构的安全性, 并推广为工业规范, 利用可信计算技术来构建通用的终端硬件平台。2003年4月, TCPA重新改组, 更名为可信计算集团(Trusted Computing Group, TCG), 并继续使用TCPA制定的“Trusted Computing Platform Specifications”。2003年10月, TCG推出了TCG 1.2技术规范。到2004年8月TCG组织已经拥有78个成员, 遍布全球各大洲。

2 可信计算系统的体系结构

2.1 可信计算的概念

“可信计算”的概念由TCPA提出, 但并没有一个明确的定义, 而且联盟内部的各大厂商对“可信计算”的理解也不尽相同。其主要思路是在计算设备硬件平台上引入安全芯片架构, 通过其提供的安全特性来提高系统的安全性。可信计算终端基于可信赖平台模块(TPM), 以密码技术为支持, 安全操作系统为核心。计算设备可以是个人计算机, 也可以是PDA、手机等具有计算能力的嵌入式设备。

“可信计算”可以从几个方面来理解: (1)用户的身份认证, 这是对使用者的信任; (2)平台软硬件配置的正确性, 这体现了使用者对平台运行环境的信任; (3)应用程序的完整性和合法性, 体现了应用程序运行的可信; (4)平台之间的可验证性, 指网络环境下平台之间的相互信任。

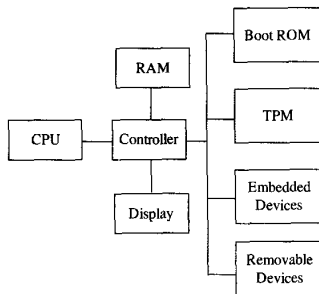


图1 含有TPM的PC平台

2.2 可信平台模块

可信平台模块(Trusted Platform Module, TPM)是可信计

作者简介: 秦中元(1974—), 男, 博士、讲师, 主研方向: 无线网络及其安全; 胡爱群, 教授、博导

收稿日期: 2005-09-23 **E-mail:** zyqin@seu.edu.cn

算平台的可信根源,从硬件底层来提供对于计算设备的保护。它是一个含有密码运算部件和存储部件的小型 SoC 片上系统,与平台主板相连,用于验证身份和处理计算机或设备在可信计算环境中使用的变量。其中主要包括微处理器、EEPROM、Flash、真随机数发生器(TRNG)等,主要完成 RSA 公钥加密/签名算法、SHA-1 安全散列算法以及安全的存储加密密钥等敏感信息。系统的所有安全认证和安全调用都通过 TPM 来完成,并建立起一条网络—应用软件—操作系统—硬件的完整的信任链关系。在信任传输的作用下,实现安全机制的整体性检查,从而确保了各环节的可信性,进而保证了整个系统的可信性。

TCG 中的密码算法包括: (1)SHA-1 散列算法,用来保证测量数据的完整性; (2)随机数产生(RNG); (3)非对称密钥生成(RSA); (4)非对称密钥加密/解密(RSA),用来保护信息的机密和对传输数据的签名; (5)对称密钥加密/解密(3DES)。

其中 RSA 和 SHA-1 是 TPM 中最基本的算法。TPM 提供公钥加密算法 RSA 对敏感数据进行加密,一般采用 1 024 位或 2 048 位的密钥。由于处理能力有限,它不提供对于大量流数据的加密,而由设备上的主处理器完成。另外,它还利用 SHA-1 安全散列算法来记录系统的测量值。

TPM 利用平台配置寄存器(PCR)来保存系统的测量记录。TPM 包含完整性测试引擎,用于采集软件和硬件的完整性相关数据,并将结果保存在 TPM 硬件的配置寄存器中。PCR 必须能够抵御来自软件和硬件的攻击。

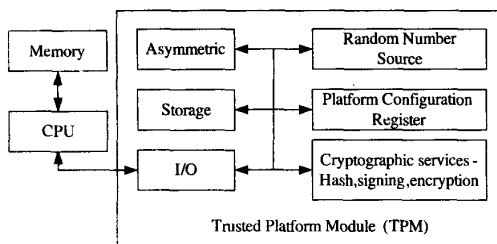


图 2 TPM 可信平台的内容

2.3 可信根和密钥管理

在 TCG 中,可信根(Root of Trust, ROT)分为: RTM(Root of Trust for Measurement), RTS(Root of Trust for Storage)和 RTR(Root of Trust for Report),分别用于用户引导和完整性测量、存储保护、记录报告的保护。

(1)RTM 是一个计算引擎,能够进行内部可靠的完整性度量。当平台开始运行时,从 RTM 开始。TPM 初始化过程包括一个 TPM 自检。通过自检可以判断 TPM 的功能是否合适。RTM 有责任选择和控制在最合适的 TPM 初始化过程。

核心测量可信根(Core Root of Trust for Measurement, CRTM)是系统启动后执行的第一段代码,它初始化可信启动顺序,执行最初的可信测量,然后引导 TPM 开始工作。CRTM 驻留在 Flash 中,必须确保不会被修改,也不会被旁路,否则系统的安全难以保证。当计算机加电或重启时, BIOS 的引导区代码检测硬件并加载操作系统,这一段代码就是 CRTM。

(2)RTS 能够维护完整性散列和散列顺序的准确值,它将完整性度量保存在日志中,将它们的散列值保存在 PCR 中。RTS 保护委托给 TPM 的密钥和数据,并管理少量活动内存,其中存放的密钥用来完成签名和解密操作。

(3)RTR 可靠地报告 RTS 保存的信息。

可信平台可以进入任何状态,不管该状态是不是安全。利用 RTM、RTS 和 RTR 测量、存储并汇报完整性测量数据,能够将平台所处的状态真实完整地报告给 TPM,再由 TPM 判断平台所处的状

态并作出合适的反应。

在 TCG 中用到多种密钥,它们都是以公钥证书的形式签发。每个可信平台模块 TPM 都有唯一的一个 EK(Endorsement Key)密钥对。EK 在 TPM 的制造过程中产生,由制造商提供。它不能用于加密或签名,只能用于解密用户认证数据或 AIK 信息从而建立平台主人。

AIK(Attestation Identity Key)用来在不泄露平台身份的情况下向另外一方证明平台的状态和配置。TPM 利用 AIK 对平台配置寄存器 PCR 进行签名。当一个平台向另外一方证明自己处于可信状态时,就向另外一方发送用 AIK 私钥加密的平台状态信息,

有效性证书:平台的所有部件都需要提供有效性证书,包括显卡、磁盘适配器、内存控制器、处理器、网卡、键盘、鼠标、各种软件等。

SRK(Storage Root Key)由平台主人创建,用来保护其它所有的密钥。SRK 和 EK 由 TPM 直接保护,它们嵌入在 TPM 中,不能被移出。

2.4 信任链的传递

信任链的传递是体现可信的重要手段,它是可信计算平台的核心机制。信任链的传递可以分为两个主要阶段: (1)从平台的加电开始到操作系统装载完毕; (2)从操作系统开始运行以及应用系统的运行。第(1)阶段信任链是单向的,而进入多任务环境下,应用的运行是随机的,信任链也成为发散的树形。具体的实现中,在第(1)个阶段可以借助简单的完整性验证手段,在第(2)个阶段可以和具体的安全规则相结合,对不同的主体定义具体的信任等级,在传递过程中按照定义的规则进行平台状态的转换。

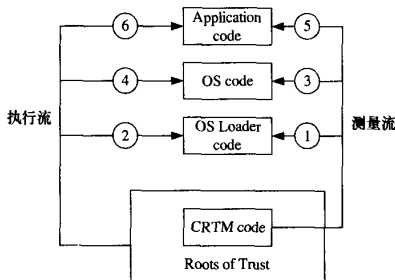


图 3 可信系统启动顺序

当系统上电启动时,系统运行程序进行上电自检,对系统的几乎所有硬件进行检测,根据 TCPA 标准,在自检过程中,所有硬件应该提供一致性数字证书(Conformance Certificate),通过它验证硬件的合法性。在载入操作系统引导记录之前, CRTM 首先检测引导系统的合法性,检测成功后载入操作系统的引导记录,将系统控制权交给引导记录,这时系统的可信区域就由 CRTM 代码扩展到操作系统的加载程序。引导记录获得控制权之后将完成系统的启动工作,这时系统的可信区域就由操作系统的加载程序扩展到操作系统。在启动程序之前,同样需要验证应用程序的身份,只有通过验证的应用程序才能正常启动,完成了这一步后,整个系统的信任区域就扩展到了应用层,从而保证了整个系统是值得信赖的。

本次的启动记录保存在平台配置寄存器 PCR 中,每次测量完系统后,对测量值和 PCR 进行如下处理:

$$PCR[n] \leftarrow SHA-1(PCR[n] + MeasuredData)$$

其中 MeasuredData 为本次的测量值,它串联在 PCR 的当前

值后面。这样,PCR保存了当前值和每次测量值的Hash码,从而保存历史记录。以前的启动记录则加密后保存在外部存储设备的日志中。

3 可信计算系统的研究现状

3.1 可信PC的研究

为了推动和支持可信计算的发展,业界许多厂商都推出了符合TCG规范的产品。2002年底,IBM发布了一款带有嵌入式安全子系统(Embedded Security Subsystem, ESS)的笔记本电脑。2003年9月,Intel正式推出了支持Palladium的LaGrande技术,LaGrande技术在个人计算机平台上构建了一个硬件安全系统,这个系统可以保护计算机数据的机密性,并防止恶意软件对计算机的攻击。微软为新的Windows平台提出下一代的安全计算基采用TCG1.2规范,为用户提供更加安全和可靠的计算环境。Infineon公司推出了以9630 TT 1.1 TPM为核心的安全解决方案。

与此同时,国内的科研机构也开展了这方面的研究。2004年6月,中国首届TCP(可信计算平台)论坛在武汉召开,国内专家、业内安全厂商对TCP进行了深入的交流。2004年8月,由国务院信息化工作办公室指导,全国信息安全标准化技术委员会主办的“可信计算标准研讨会”在北京召开。国际TCG(可信计算集团)的主要成员单位专家、国内相关企业单位、科研机构出席了本次研讨会,并以安全芯片及安全PC、操作系统及应用系统软件、网络两个主题为讨论小组进行了互动式交流。

依托武汉大学技术力量的武汉瑞达科技有限公司,同TCG的思路非常相似,瑞达提出的技术框架也是在主板上增加安全控制芯片以及从BIOS入手来增强平台的安全性,不同的是没有引入内涵更为丰富的可信机制。联想是率先加入TCG的国内厂家,在PC整机设计制造方面有着丰富的经验,同时它们还和英特尔公司合作成立了联合实验室研究可信计算技术,并且有望在未来的PC平台生产上采用LT技术。联想集团预测,2006年中国将有60%左右的PC机主板附有安全芯片。

3.2 可信移动设备的研究

TCG组织提出可信计算系统的概念以来,又针对不同的设备定义了具体的TPM,例如针对PC机、PDA、手机等。目前移动设备已经变得更加智能,处理能力也日益提高,它

们已经具备了现代PC机的许多功能。固定互联网和移动互联网之间的融合也产生了移动设备安全的问题。因此如何保证移动计算的可信问题就摆在了我们面前。

移动设备与台式机、路由器等固定设备相比,除了具有携带方便、操作简单等优点,还具有以下特点:计算能力比较低,存储空间小,显示分辨率低,数据输入不方便,功率约束强等。另外,它们一般仅采用无线上网。对于移动设备来说,安全所带来的体积大小和成本是最关键的因素。

针对移动计算的这些问题,TCG专门成立了手机工作组,计划在2005年推出针对可信计算的移动安全规范。另外,2004年10月,IBM、Intel、NTT DoCoMo在可信计算的基础上,提出了可信的移动计算平台(Trusted Mobile Platform, TMP),该规范分别对硬件、软件和通信协议对移动可信计算提出了要求,其硬件架构采用了两个处理器:一个为应用程序处理器,负责运行操作系统和管理所有的设备,包括TPM;另一个为通信处理器,负责处理射频发送及与SIM卡的接口。

4 结语

随着各种入侵手段和黑客技术的迅速发展,传统的信息防御技术已经不能满足系统安全的需要,因此可信计算系统的研究被提上了议事日程。它通过在计算设备上安装可信平台模块,以信任链的方式保证计算设备的安全,大大增强了计算设备在数据安全存储、平台真实性、完整性证明等方面的能力,对信息安全技术及产业将产生深远的影响。

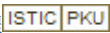
参考文献

- 1 TCG Specification Architecture Overview Specification (Revision 1.2)[Z]. https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf, 2004.
- 2 余发江, 张焕国. 可信安全计算平台的一种实现[J]. 武汉大学学报, 2004, 50(1): 69-73.
- 3 Trusted Mobile Platform Specification Hardware Architecture Description[Z]. http://www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf.
- 4 Trusted Mobile Platform Specification Software Architecture Description[Z]. http://www.trusted-mobile.org/TMP_SWAD_rev1_00.pdf.
- 5 谭兴烈. 可信计算平台中的关键部件 PTM[J]. 信息安全与通信保密, 2005, (2): 29-31.
- 6 Krawczyk H. Simple Forward-secure Signatures from Any Signature Scheme[C]. Proc. of the 7th ACM Conference on Computer and Communication Security, 2000-11: 108-115.
- 7 Malkin T, Micciancio D, Miner S. Composition and Efficiency Tradeoffs for Forward-secure Digital Signatures[C]. Proceedings of Eurocrypt, 2002.
- 8 Kang B G, Park J H, Hahn S G. A New Forward Secure Signature Scheme[Z]. <http://citeseer.ist.psu.edu/700468.html>.

(上接第110页)

- 3 Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C]. Proc. of Crypto'99. Springer-Verlag, 1999: 431-448.
- 4 Abdalla M, Reyzin L. A New Forward-secure Digital Signature Scheme[C]. Proc. of Advance in Cryptology——ASIACRYPT. Springer-Verlag, 2000: 116-129.
- 5 Itkis G, Reyzin L. Forward-secure Signatures with Optimal Signing and Verifying[C]. Proc. of CRYPTO'01. Springer-Verlag, 2001: 332.

可信计算系统及其研究现状

作者: 秦中元, 胡爱群, QIN Zhongyuan, HU Aiqun
作者单位: 东南大学无线电工程系, 南京, 210096
刊名: 计算机工程 
英文刊名: COMPUTER ENGINEERING
年, 卷(期): 2006, 32(14)
引用次数: 9次

参考文献(5条)

1. TCG Specification Architecture Overview Specification (Revision 1.2) 2004
2. 余发江, 张焕国 可信安全计算平台的一种实现[期刊论文]-武汉大学学报(理学版) 2004(1)
3. Trusted Mobile Platform Specification Hardware Architecture Description
4. Trusted Mobile Platform Specification Software Architecture Description
5. 谭烈烈 可信计算平台中的关键部件TPM[期刊论文]-信息安全与通信保密 2005(2)

相似文献(3条)

1. 期刊论文 叶宾, YE Bin 增强可信计算平台模块的可信度 -信息安全与通信保密2009(7)
为建立安全的计算环境, TCG提出了可信计算系统, 目前已经逐步得到广泛的认可和应用. TPM作为TCG组织推出的可信计算平台的可信“根”和核心, 起着最重要的作用. 文章通过分析现有TPM存在的一些安全隐患, 可以找到一些办法并增强TPM的可信度.
2. 期刊论文 肖政, 韩英, 刘小杰, 华东明, 侯紫峰, XIAO Zheng, HAN Ying, LIU Xiao-jie, HUA Dong-ming, HOU Zi-feng
基于可信计算平台的接入认证模型和OIAP授权协议的研究与应用 -小型微型计算机系统2007, 28(8)
在参考现有认证技术的基础上, 提出了一种基于可信计算平台的可信接入认证模型. 利用此模型可以及时发现待接入设备是否是安全可信, 然后进行正确处理. 在确定接入的设备是安全可信后, 考虑到下一步此设备需要使用认证授权协议OIAP向服务资源发出申请, 但是OIAP协议本身存在基于口令机制的缺陷, 为此本文还提出增强OIAP协议安全性的方法. 在“八六三”项目“可信计算系统平台”中的实际应用证明上述的模型和方法的有效性, 并展现了其良好的应用前景.
3. 期刊论文 肖政, 韩英, 叶蓬, 侯紫峰, XIAO Zheng, HAN Ying, YE Peng, HOU Zi-feng 基于可信计算平台的体系结构研究与应用 -计算机应用2006, 26(8)
介绍了可信计算平制, 以及目前可信计算平台的研究进展情况, 分析了基于可信计算平台技术的应用前景和存在的问题, 并对未来的趋势进行了展望. 基于863项目“可信计算系统平台”的安全芯片研制成功, 展现了可信计算的良好应用前景.

引证文献(9条)

1. 林劼, 李晓哲, 戴一奇 一种可信局域网计算环境原型系统的实现[期刊论文]-北京电子科技学院学报 2008(4)
2. 何宇, 吕光宏, 敖贵宏 可信计算及其对Ad Hoc网络安全的启发[期刊论文]-计算机安全 2008(04)
3. 李霏, 王让定, 徐霁 内嵌TPM的视频监控服务器安全方案[期刊论文]-安防科技 2007(10)
4. 王勇 基于可信计算的网内网监控系统的应用研究[期刊论文]-广西质量监督导报 2007(06)
5. 李霏, 王让定, 徐霁 内嵌TPM的视频监控服务器安全方案[期刊论文]-微电子学与计算机 2007(09)
6. 章睿, 刘吉强, 彭双和 基于EFI的信任链传递研究及实现[期刊论文]-计算机应用 2007(09)
7. 魏乐, 叶剑新, 黄健 可信计算的初步研究[期刊论文]-科技资讯 2007(13)
8. 樊静淳 论可信计算的研究与发展[期刊论文]-济南职业学院学报 2007(03)
9. 靳蓓蓓, 张仕斌 可信计算平台及其研究现状[期刊论文]-长春大学学报(自然科学版) 2007(02)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_jsjgc200614041.aspx

下载时间: 2009年12月21日