

可信计算之信任链技术研究

王江少, 余 综, 李 光

(华北计算技术研究所, 北京 100083)

摘 要: 可信计算近年发展迅速, 被认为是最有可能从根本上解决计算机系统安全问题的一种方案, 不同于传统信息安全解决办法, 它以新的思路即主动防御来解决计算机和网络系统的信息安全问题。信任根和信任链是可信计算的根本组成部分。介绍了可信计算及信任链的相关知识, 介绍了信任根, 可信认证机制。最后详细给出了基于 PCI 扩展 ROM 的可信计算之信任链部分链实现的可行方案。

关键词: 可信计算; 信任根; 信任链; 可信认证; PCI 扩展 ROM

中图分类号: TP393.08 **文献标识码:** A **文章编号:** 1000-7024(2008)09-2195-04

Study of trusted chain technology of computing trusted

WANG Jiang-shao, YU Zong, LI Guang

(North China Institute of Computing Technology, Beijing 100083, China)

Abstract: Trusted computing, which has been considered as the best method in resolving the security of computer system, has been developing very fast in recent years. It is a new measure that makes use of active defending to resolve security problem of computer and network system. Root of the trust and the system of trusted chain are the most important components of trusted computing. The trusted computing and the trusted chain system, as well as the device of root of trust, and the authentication mechanism of trusted computing are introduced. At last a feasible scheme of trusted chain system based on PCI extended ROM used to resolve part of chain is provided in detail.

Key words: trusted computing; root of trust; trusted chain; trust authentication; PCI extended ROM

0 引 言

由于传统计算机操作系统、网络协议等在体系结构设计上存在先天不足, 使得现今的计算机和网络系统存在着严重的安全隐患。利用这些安全隐患, 病毒和黑客的攻击手段千变万化, 严重威胁到了国家、政府、公司企业以及个人单位等信息数据的安全。通常的信息安全建设是一种被动防御的发展思路, 实现计算机的安全基本上都是通过在计算机和外部世界之间增加一些安全层次。

因此, 每出现一种新的病毒或攻击方法, 就必须增强某些安全层或者增加一个新的安全层, 这样就需要不断的升级防火墙、病毒特征库等, 使得安全投入不断膨胀, 维护和管理也变得复杂和难以实施。然而这种方法仅能修补已造成的破坏, 并不能解决根本的问题。为了解决计算机系统结构上的不安全问题, 从根本上提高其安全性, 可信计算, 一种主动防御的发展思路应运而生。

可信计算通过建立可信的计算机系统和可信的网络系统, 保证提供可信的服务、可信的计算, 使得每个使用者、每台设备终端它们的每个重要操作都必须通过授权和认证, 并留

下操作日志, 保证源头的安全性。可信计算的提出, 为计算机安全提供了一个新的发展方向。

从理论上讲, 国际可信计算工作组(TCG)组织的可信计算技术规范强调从硬件芯片级别到软件应用的逐级认证、逐级信任思想; 强调可信的信任根芯片 TPM (trusted platform module)在计算机系统开机加电伊始, 对硬件芯片、连接外设和系统 BIOS(basic input and output system)代码进行完整性测量和认证, 其后建立信任链, 在 TPM 信任根的功能支撑下, 逐级认证到上层应用。信任链的建立主要体现在通用操作系统中可信软件栈的设计实现。

从工程实践上看, 国际厂商 IBM 等推出了搭载 TPM 芯片的计算机系统, 国内厂商瑞达推出了配置 TPM 芯片、可信主板等可信特征的可信计算机。但是, 前者的 TPM 芯片主要用于数据加密保护, 未实现完整性测量和信任链传递等关键功能; 后者对部分硬件、外设和数据实现了完整性测量, 也未实现信任链传递的功能。所以, 从本质特征上并未实现具有信任根和信任链的高可信计算机系统。

鉴于此, 本文通过对信任链的研究, 提出一个实现信任链部分链的可行方案。

收稿日期: 2007-06-07 E-mail: wangjiangshao@163.com

作者简介: 王江少(1983—), 男, 湖南耒阳人, 硕士研究生, 研究方向为信息安全和嵌入式系统软件设计; 余综(1972—), 男, 正研级高级工程师, 研究方向为计算机体系结构; 李光(1976—), 男, 硕士研究生, 研究方向为嵌入式操作系统。

1 可信计算研究现状

可信计算,按照国际可信计算工作组(TCG)的定义,是一种期望,在这种期望下设备按照特定的目的以特定的方式运转。可信计算技术的核心是一个称为可信平台模块(TPM)的安全芯片,该芯片是一个含有密码运算部件和存储部件的系统级芯片,以密码技术为支持、安全操作系统为核心,涉及到身份认证、软硬件配置、应用程序、平台间验证和管理等内容。一个可信的计算机系统由可信硬件平台、可信操作系统和可信应用组件组成。

信任根和信任链是可信计算机系统的重要特征和关键组成部分。信任根是可信计算系统可信的起点,它必须具有高安全和高可信性,它的可信性由物理安全和管理安全确保。信任链是用于传递可信的方式,用于把信任从信任源点传递到整个系统。

可信计算平台的基本思路是:首先构建一个信任根,再建立一条信任链,从信任根开始到硬件平台、到操作系统、再到应用、一级认证一级、一级信任一级,从而把这种信任扩展到整个计算机系统。

可信计算发展迅速,下面讲述其国内外发展现状。

在国外,至20世纪70年代初期,Anderson JP首次提出可信系统的概念,由此开始了对可信计算机系统的研究。1999年,由Intel、Compaq、HP、IBM和Microsoft等国际著名企业发起成立了一个“可信计算平台联盟TCPA(trusted computing platform alliance)”。该组织致力于促成新一代具有安全、信任能力的硬件运算平台。到2003年,TCPA组织重组为“可信计算组”TCG(trusted computing group)。TCG组织在原TCPA组织强调安全硬件平台构建的宗旨之外,更进一步增加了对软件安全性的关注,旨在通过使用硬件模块组件和跨平台的软件接口来构筑更安全的计算环境,促进统一的可信计算平台工作标准的制定。

在国内,可信计算技术研发工作已经起步,发展很快,并成为信息安全领域的关注热点。瑞达、联想、兆日等厂商先后参加国际TCG组织,积极参与国际交流;在产品研发方面也有一定的突出表现,如:2004年10月瑞达公司研制的、专注于终端安全的国内首款可信计算平台系统通过了技术鉴定;12月,天融信公司推出了致力于可信网络平台(TNP)的可信安全管理平台和可信安全系统平台;联想方面也宣称在可信主机、可信网络和可信管理系统3个方面取得了重要技术发展。

可信计算技术已经成为计算机信息安全技术新的发展趋势。但是,可信计算技术目前还是在概念推广和技术体系发展的阶段,完全符合有关TCG组织可信计算规范的产品、达到使用程度,并得到市场肯定的产品还非常少。而信任链技术是实现可信计算系统的关键技术之一,通过对它的研究将有利于产生可信计算机产品的进程。

2 信任链技术

信任链是可信计算机系统的一个关键组成部分,是可信计算技术存在非常有力的思想。它的存在保证了计算机系统从可信源头开始至系统启动整个过程的安全可信性。

TCG提出信任链,是以信任根TPM芯片为核心(提供密码操作和安全存储),起点为CRTM(core root of trust module,核心信任根模块)。CRTM可以看成是引导BIOS的程序,是一段简单可控的代码模块,认为其绝对可信。从加电开始,CRTM引导BIOS并验证BIOS的完整性,如果BIOS代码段完整没有被篡改,就说明BIOS与最初的状态一致,因此认为其是安全的,则把CPU控制权交给BIOS代码。BIOS运行其代码,进行计算机硬件的初始化,当BIOS运行即将结束且需要递交CPU控制权时,它要验证OS Loader的完整性,确保其没有被篡改过,是安全的,验证通过之后再吧CPU控制权交给OS Loader代码。类似的,再到OS,再到应用程序,这样以一级验证一级,一级信任一级的方式,实现了信任链的传递,最终形成一个可信的运行环境,从根本上保证了计算机系统的安全性。

图1是TCG所采纳的信任链传递的简单示意图,基本上体现了信任链的思想。

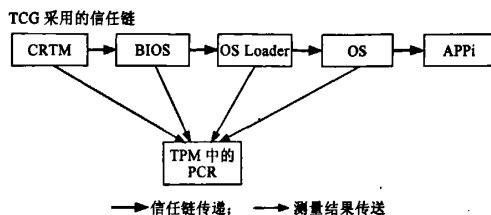


图1 TCG采用的信任链

信任链的两个重要组成部分,信任根和它的链传递机制即可信认证。下面对它们分别进行介绍。

2.1 信任根

计算机信任根是可信计算机系统的信任基点,是信任链的核心,还是所有系统行为完整性的测量基础,必须保证自身的高安全性和高性能。

TCG定义了一个叫做可信平台模块(trusted platform module, TPM)的芯片设备作为受保护活动的“信任根”,TCG认为如果从一个初始的“信任根”出发,在平台计算环境的每一次转换时,这种信任状态可以通过传递的方式保持下去不被破坏,那么平台上的计算环境始终是可信的,在可信环境下的各种操作也不会破坏平台的可信,平台本身的完整性得到保证,终端安全自然也得到了保证,这就是信任链的传递机制。

TPM实际上是一个含有密码运算部件和存储部件的小型片上系统,它提供了一系列密码处理功能,如RSA加速器、SHA-1算法引擎(HASH:散列算法模块)、RTC(随机数发生器)以及存放密钥等关键信息的NVRAM等。这些功能在TPM硬件内部执行,只提供I/O接口,TPM外部的硬件和软件代理不能干预TPM内部密码函数的执行。

BIOS是计算机启动最先执行的一段程序代码。它首先是进行POST(power-on self test,加电自检),检测系统中一些关键设备是否存在以及其能否正常工作,例如,内存和显卡设备。然后BIOS测试所有内存,检测系统中安装的一些标准硬件设备,包括硬盘、CD-ROM、串口、并口、软驱等。再是,系统BIOS将开始检测和配置系统中安装的即插即用设备,同时为设备分配中断、DMA通道和I/O端口等资源。系统BIOS的最

后一项工作是根据用户指定的启动顺序从软盘、硬盘或光驱启动操作系统。BIOS 代码的执行是计算机系统非常重要的一环,它基本上实现了计算机硬件检测、配置和初始化。正因为 BIOS 是计算启动最先执行的代码,所以它的可信执行是可信计算的基础。幸运的是 BIOS 的发展历史以及 BIOS 生产厂商的信誉,使得就连国际 TCG 也认为 BIOS 是可信的,因此在实现可信计算的过程中不对其实施可信验证(逻辑上是一定要要进行可信认证,所以文章提供了其实现方案),它和 TPM 共同构成可信计算机系统的信任根。

在讲述通过扩展 BIOS,增加 PCI 扩展 ROM^[7]实现信任链传递方案之前,先介绍可信计算中信任传递的实现机制,即可信认证。

2.2 可信认证

信任链传递就是通过一级认证一级,达到一级信任一级的过程,以至把这种信任扩展到整个计算机系统。其中可信认证是通过模块的完整性认证来实现的。

那么完整性认证能够实现可信认证,达到信任在链中的传递吗?针对这个问题,首先得弄清一点,就是软件的来源。这里存在一个假设,即如果软件的来源正规,它的提供者信誉很好,并且提供有该软件足够的测试证明,这样就认为该软件是可信的。因此在最初获得该软件的时候,通过信任根提供的密码接口功能,计算它的完整性基准值,并把这个基准值存储到信任根的安全存储区中,供以后的完整性认证使用。当进行完整性认证时,如果计算出的值和存储在信任根中的基准值相符,说明该软件在使用过程中没有被篡改过,和最初软件一致,于是认为该软件是可信的,因此对于它所提供的功能也认为是可信的。

可信认证过程分为两个方面:

(1)完整性基准值的建立。在建立信任链的过程中,首先需要产生各个阶段关键文件或软件的完整性认证基准值,用于以后在可信认证中作为一个认证基准,然后把这些基准值存储到信任根的安全存储区域中。如果以后用户或者系统通过授权(通过授权则认为此改动是安全可信的)更改了某些关键文件或软件信息,需要对这些改动了的关键文件或软件调用信任根提供的密码功能重新计算其完整性基准值。这样以后每次进入系统时,就可以实施系统的完整性认证,以达到系统的可信认证。

(2)完整性认证,实现信任传递的过程。有了完整性基准值,系统就可以实施完整性认证。完整性认证就是通过对实体实施认证计算,这种计算和生成完整性基准值的方法一致,然后把结果值与基准值进行比较,来达到认证的过程。如果认证失败,即两次得到的结果不一致,说明被认证的实体对象被修改过,而且这种修改没有得到授权,因为得到授权的修改会重新计算完整性基准值。失败则通知用户,由用户根据具体情况进行处理。如果认证成功,说明被认证实体完好,没有被篡改,因此认为该实体可信,可以实施 CPU 控制权的交接,实现信任的安全传递。

3 信任链实现可行方案

通过对可信计算的分析和理解,在没有出现 TPM 大规模

生产,且 PCI 设备已经大量普及的情况下,为保护用户的现有投资,结合计算机 BIOS 本身的可扩展性,文章提出了基于 PCI 扩展 ROM^[7]来实现信任链部分链传递的可行方案。其主要思想是通过改造现有的通用 PC 机,利用现有的安全手段,实现一个安全可信的计算机。

方案没有更改现有 PC 机的体系结构,如图 2 所示,通过增加一个改造的 PCI 设备(称之为 PCI TPM),实现简单的密码功能和安全存储,其和计算机 BIOS 共同构成计算系统的信任根,形成信任源点。扩展 BIOS,利用 PCI 扩展 ROM,实现 BIOS 的可信认证以及 OS Loader 的可信认证。该信任链中没有 TCG 提出的 CRTM 设备,不过其中的 PCI 扩展 ROM 设备基本实现它的功能。下面几节对可行方案进行了详细具体的描述,它包括信任根的建立,以及 BIOS 和 OS Loader 的可信认证等,关于 OS 以及应用程序级的可信认证是我们进一步要研究的目标。

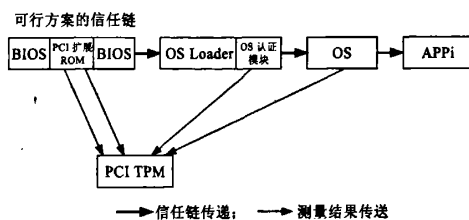


图 2 可行方案的信任链

3.1 建立信任根

信任根是可信计算技术的核心,也是信任链的信任源头。现有通用 PC 体系结构,PCI 总线是其不可或缺的一种技术,PCI 设备非常普及。因此,文章提出通过提供一个具有与 TCG 提出的 TPM 类似功能(必要的密码算法、安全存储)的 PCI 设备来实现 TPM 功能,称之为 PCI TPM,其在技术上实现是完全可行的。PCI TPM 和计算机 BIOS 共同构成计算机系统的信任根。这个 PCI 设备,方案采用计算机安全模块^[8],它来自于安全模块项目成果。

安全模块项目是 2001 年信息产业部电子信息产业发展基金重点招议标项目,安全模块的设计综合了可信计算、嵌入式技术等诸多思想,形成一套解决计算机系统安全、网络安全、数据安全的完整解决方案。安全模块的全称为计算机安全控制模块,已经申请相应的专利保护(专利申请号:2005100005555.7)。

计算机安全模块提供了丰富的密码功能接口,以及其拥有自己的存储区域。它通过 PCI 总线接口与主机连接,当用户需要安全计算机的时候,在现有的计算机上插入一块计算机安全模块就组成了一台安全计算机,从而保护了用户的现有投资。

方案通过采用计算机安全模块来实现 PCI TPM,再结合计算机 BIOS 实现可信计算机的信任根设备。和 TCG 提出的可信计算机不同,它不需要对现有的 PC 机进行体系结构上的改造,仅仅为其增加一个 PCI 设备,非常便利和实用。

3.2 BIOS 的可信认证

在计算机的启动过程中,当 POST 检测到 PCI 扩展 ROM

后,就会复制恰当的映像到RAM中,并执行其初始化代码用来完成设备的初始化。PCI扩展ROM中映像的初始化代码是该可行方案能够实施的关键。通过在该初始化代码中增加对BIOS的可信认证代码,就能够实现对BIOS的可信认证。

BIOS代码,在计算机系统中以固件形式存在,存放在计算机系统ROM(只读存储芯片)或者EPROM,EEPROM中,根据这些存储介质本身的特性,即使在计算机关机或者系统掉电后,数据也不会丢失。在x86平台下,整个计算机系统的BIOS代码被映射到地址空间范围C0000H-FFFFFH内,这是x86平台本身约定的。由于BIOS地址空间的相对固定,并且其代码数据是只读的,因此可以通过在PCI扩展ROM中对该地址段中数据实施完整性认证,确认该地址段中数据没有被篡改过,达到对BIOS代码的可信认证。PCI扩展ROM一般也是被映射到C0000H-FFFFFH范围之内,因此我们把这种借助PCI扩展ROM实现BIOS可信认证的方式称为BIOS自认证方式。如果BIOS的完整性出现问题,说明BIOS被修改过,且这种修改没有得到授权,因为授权的修改会重新计算代码数据的完整性基准值。通过度量报告通知用户,由用户根据实际情况做相应处理。

3.3 OS Loader的可信认证

在PCI扩展ROM中实施BIOS的认证,同样也可在其中实施OS Loader的可信认证。普通PC中,OS Loader处于BIOS和OS之间,主要职责就如其名一样,用于引导操作系统,并把CPU控制权递交给它。鉴于当前引导程序GRUB^[9](GRand unified boot loader)比较流行,使用方便且是开源的,源代码可以获得,文章方案选择GRUB作为OS Loader进行研究。

GRUB代码编译后生成两个模块,stage1和stage2。生成stage1的代码基本上是由汇编程序编写,生成stage2的代码基本上都是由C语言编写的。stage1功能主要是完成stage2模块的引导和维护计算机系统的MBR(master boot record,主引导记录,硬盘物理位置上的第一个扇区)分区表以及BIOS参数块。Stage2模块基本上是由C语言编写的代码,它提供了复杂且灵活的功能,为用户提供更多的选择,方便了用户的使用。它还提供了像Linux控制台一样与用户交互的控制台界面,在该控制台下可以实施一些操作系统设置和操作,但总的来说stage2模块的核心任务就是引导操作系统。

因此,实施对GRUB的完整性认证就涉及到它的关键模块stage1和stage2。通过对stage1和stage2的完整性验证来完成对GRUB的完整性认证。以磁盘引导为例,stage1和stage2存储在磁盘上,又由于OS还没有被引导起来,不存在文件系统,所以实施对stage1和stage2的验证需要通过它们在磁盘的物理位置来实现。读取磁盘物理位置上的块数据,可以通过BIOS提供的读写磁盘INT 13H(可以选择基本的INT 13H,也可以选择扩展的INT 13H,根据具体的情况来确定)功能调用完成。而stage1和stage2的物理位置怎么确定呢?通过分析GRUB源代码,发现stage1模块存放在磁盘的第一个物理扇区内,即取代了原来的MBR。BIOS代码把CPU控制权递交给OS Loader,实质上进行的操作就是读取磁盘引导介质上的第一个扇区到内存,并运行它,这是平台硬性规定的实现方式。

因此stage1模块的物理位置问题解决了,但stage2模块呢?stage1模块的主要任务就是引导stage2模块,显然就得从stage1入手。分析发现,在系统安装GRUB的时候,就建立了stage1和stage2的联系。通过stage1的分区表可以找到stage2模块第一个扇区所在的位置,然后在通过这个扇区可以找到所有的stage2的其它扇区。至此就完成stage1和stage2的物理定位问题。这样就可以实施对它们的可信认证了。

PCI扩展ROM可以一步一步的实现系统引导程序GRUB即stage1和stage2的完整性认证,实现OS Loader的可信认证,完成信任的进一步传递。

4 结束语

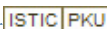
可信计算是解决信息安全问题中一种新思路的代表,它提出实施主动防御的策略,从计算机端点来保证安全的源头。它是现今安全领域中的研究热点,被认为是最有可能成为从根本上解决计算机系统安全问题的方法。信任根和信任链是可信计算方法思想的根本体现和灵魂。通过在计算机系统中实现信任根和信任链就基本上完成了通用计算机系统的可信改造。

本文通过介绍可信计算概念、发展历史,以及介绍信任链技术,信任根,以及信任传递机制。最后提供了实现信任链部分链传递的可行方案,使得我们在研究可信计算,以及信任链的过程中有了一个比较清晰方向。根据当前PC机的大量普及,PCI设备的通用性,为更好的保护用户的现有投资,文章可行方案,通过了采用PCI设备,利用安全模块项目的成果计算机安全模块来建立的信任根,提出了在PCI扩展ROM实现BIOS可信认证和OS Loader(选择GRUB)可信认证。文章仅仅提出了实现可信计算信任链中部分链传递的可行方案,即BIOS的可信认证和OS Loader的可信认证,关于OS的可信认证以及应用程序的可信认证,以及实现方式将是我们进一步要研究的目标。

参考文献:

- [1] 陈钟,刘鹏,刘欣.可信计算概论[J].信息安全和通信保密,2003(11):17-19.
- [2] 候方勇,周进.可信计算研究[J].计算机应用研究,2004,21(12):1-4.
- [3] 谭兴烈.可信计算平台中的关键部件TPM[J].信息安全与通信保密,2005(2):39-41.
- [4] 沈昌祥.可信计算平台与安全操作系统[J].网络安全技术与应用,2005(4):9-10.
- [5] Laurence Bonney. 引导程序之争:了解LILO和GRUB [DB/OL]. <http://www-128.ibm.com/>, 2005.
- [6] 李娜.可信计算与内网安全[J].计算机安全,2005(10):10-112.
- [7] Ravi Budruk, Don Anderson, Tom Shanley, et al. PCI Express 系统体系结构标准教材[M]. 田玉敏,王崧,张波,等译.北京:电子工业出版社,2005:512-524.
- [8] 李光,余综.嵌入式设备在可信领域中的应用研究[J].计算机工程与应用,2006,41(增刊):140-144.

可信计算之信任链技术研究

作者: [王江少](#), [余综](#), [李光](#), [WANG Jiang-shao](#), [YU Zong](#), [LI Guang](#)
作者单位: [华北计算技术研究所, 北京, 100083](#)
刊名: [计算机工程与设计](#) 
英文刊名: [COMPUTER ENGINEERING AND DESIGN](#)
年, 卷(期): 2008, 29(9)
引用次数: 1次

参考文献(8条)

1. 陈钟, 刘鹏, 刘欣 [可信计算概论](#)[期刊论文]-[信息安全与通信保密](#) 2003(11)
2. 侯方勇, 周进, 王志英, 刘真, 刘芸 [可信计算研究](#)[期刊论文]-[计算机应用研究](#) 2004(12)
3. 谭兴烈 [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)
4. 沈昌祥 [可信计算平台与安全操作系统](#)[期刊论文]-[网络安全技术与应用](#) 2005(4)
5. Laurence Bonney [引导程序之争: 了解LILO和GRUB](#) 2005
6. 李娜 [可信计算与内网安全](#)[期刊论文]-[计算机安全](#) 2005(10)
7. Ravi Budruk, Don Anderson, Tom Shanley, et al. 田玉敏, 王崧, 张波 [PCI Express系统体系结构标准教材](#) 2005
8. 李光, 余综 [嵌入式设备在可信领域中的应用研究](#) 2006(zk)

相似文献(10条)

1. 期刊论文 林小茶, 李光, LIN Xiao-cha, LI Guang [基于嵌入式技术的信任根研究](#) -[计算机工程与应用](#)2007, 43(16)
可信计算近年来发展迅速, 被认为最有可能从根源上解决计算机的安全问题, 信任根是可信计算的根。简要介绍了可信计算的发展历史, 分析了可信产品市场不景气的原因, 从可信计算信任根的角度入手, 提出了两种采用嵌入式技术来实现信任根的方案, 并给出了方案的详细设计思想。
2. 期刊论文 林小茶, 李光, 金爽, LIN Xiao-cha, LI Guang, JIN Shuang [嵌入式可信计算机研究](#) -[计算机工程与设计](#) 2009, 30(16)
将可信计算技术应用到嵌入式系统中, 是一条有效解决嵌入式设备安全问题的新思路。首先阐述将可信计算与嵌入式技术相结合的趋势, 然后分析了该技术所面临的诸多挑战, 并给出了将CRTM集成到嵌入式TPM中实现的嵌入式可信计算机体系结构, 最后分别从信任根和信任链两方面提出了满足嵌入式系统需求的详细设计方案。
3. 学位论文 毛健 [可信计算模式研究与模块实现](#) 2006
随着信息技术和网络技术的普及和发展, 信息安全的需求已经越来越迫切, 而传统的个人计算平台体系架构存在着诸如数据物理安全、访问权限控制以及双端通信安全等威胁, 为了消除这些固有安全缺陷, 本论文引入了可信计算的研究课题, 系上海市科委重大科技攻关项目“高性能信息安全SoC平台”的一部分。在文中, 作者综合研究和参考了目前流行的多种可信计算思想, 首先设计了平台信任的建立和传递机制, 规定了三大信任根RTM/RTS/RTR, 采用信任链传递、信任域扩展的方式建立可靠的信任体系, 并在此基础上构建了一种简单、可靠、易于实现的可信计算模型体系。它包含有可信的存储, 平台配置信息分析、存储, 以及平台完整性报告三大功能, 并围绕这三个功能构建了包含算法、协议和命令在内的一套完整的可信计算模式, 该模式与现有计算平台配合工作, 可以为个人计算机提供机密信息的硬件绑定封装、防非法用户访问、防越权操作以及集团化的it管理性能。另一方面, 本文给出了可信计算模式的完整RTL实现, 它既包括了硬件的总体构架、地址分配、模块接口时序等, 还包含了一套完整的固件用于运行状态转换和命令处理, 并和上层驱动进行接口, 提供层次化的功能。本文的最后给出了最终实现的芯片版图数据以及固件主要命令列表。
4. 学位论文 童永清 [基于智能卡和PKI的可信计算平台的研究与实现](#) 2008
当前, 网络安全形势日趋严峻的一个重要原因是网络中充斥着大量含有漏洞和弱点的隐患终端。这些隐患终端不仅会成为被攻击的对象, 还可能被攻击者利用, 成为黑客攻击、病毒传播的中介和跳板, 从而使整个网络处于不安全的状态之下。隐患终端之所以会引起如此严重的安全问题, 从本质上来说是因为现有的安全技术无法保证终端系统的程序执行环境是可以被信任的。如果终端系统上关键的软硬件配置无法被恶意篡改, 应用程序的行为始终是可预期和可控的, 那么系统的安全性将大大提高, 而且对恶意代码和黑客攻击具有一定的免疫性。为了应对隐患终端所引起安全问题, 学术界提出了可信计算这一概念。可信计算技术保证在主机上所实施行为都是可预知和可控制的。可信计算技术确保主机具有机密性、完整性、可控性、和抗抵赖性。可信计算技术的基本思路是, 首先构建一个信任根, 信任根由密码技术和物理安全来保证其始终是可信的, 然后从信任根开始到硬件平台、操作系统、应用程序建立一条信任链, 一级认证一级, 一级信任一级, 从而把这种信任扩展到整个计算机系统, 乃至一个网络。在可信计算组织提出的可信计算平台框架和可信网络架构的基础上, 提出并实现了使用智能卡和PKI技术来构建可信计算平台和建立可信网络连接。该平台可保证上层的应用程序, 如Java程序, 始终是可信的。本文的主要贡献有: 1) 使用基于PKCS#11标准的智能卡作为信任根。该类型的智能卡不仅具有一般信任根所必需的安全存储和密码运算功能, 而且由于其基于PKCS#11标准和带有USB接口, 因此使用上更为方便, 价格上更为便宜。以该信任根为基础, 通过建立一条信任链构建了可信主机。具体做法是, 收集终端系统各硬件的特征信息, 将其存储于信任根中。在系统启动时, 逐级验证各硬件的特征值, 保证系统是可信的。2) 参照可信计算组织提出的可信网络模型, 设计并实现了一个分层的可信网络体系结构。该体系结构分为三层, 底层为使用OpenSSL开源库构建的CA, 该CA用于为各终端系统签发表征其唯一身份的证书; 中层为一个可信网络认证协议; 上层是一个完整性信息收集器, 该收集器用于收集表征终端系统唯一身份的信息, 该信息是数字证书的重要组成部分。3) 设计并实现了一个可信网络认证协议。该协议用于完成客户端和服务端通信前的认证, 保证只有可信的主机才能接入和访问网络, 保证了网络中主机的不可抵赖性和可信性。
5. 期刊论文 方艳湘, 黄涛, FANG Yanxiang, HUANG Tao [Linux可信启动的设计与实现](#) -[计算机工程](#)2006, 32(9)
可信计算组织(TCG)提出了可信计算规范, 其主要思想就是通过度量和保障组成平台的各组件的完整性来保证平台及应用的安全。启动过程是操作系统的基础, 因此实施可信启动对操作系统意义重大。基于Linux启动的现实条件, 结合TCG规范中可信度量和可信链的思想, 利用TPM提供的可信计算和保护存储功能, 设计了Linux可信启动过程TSPL, 并实现了原型。设计中充分考虑到启动过程的复杂性和度量数据的多样性, 不仅度量了程序代码, 还对影响执行程序行为的配置文件和环境数据进行了度量。

6. 会议论文 [曾颖明, 刘向东](#) [UEFI架构下BIOS安全增强技术](#) 2008

UEFI是最新一代BIOS技术,越来越受到人们的重视,概况了当前的发展状况,并分析了其相对传统BIOS的优势,对UEFI Framework(UEFI架构)、实现机制、安全漏洞和加载过程中的安全风险进行了研究,指出UEFI当前存在的几个安全问题,针对这些问题研究UEFI架构下BIOS安全增强技术.

7. 期刊论文 [陈书义, 闻英友, 赵宏, CHEN Shu-yi, WEN Ying-you, ZHAO Hong](#) [基于模糊集合的可信计算信任模型评估](#)

-[计算机科学](#)2008, 35 (11)

可信计算是信息安全的重要研究领域,而信任模型的可信性评估是该领域中亟待解决的关键问题.在深入研究可信计算信任根、信任链及其可信性影响因素的基础上,提出了基于模糊集合理论的可信计算信任模型评估方法.基于模糊集合理论的评估方法定义了不同的可信度度量规则和模糊集合,基于计算得到的可信度,评价信任模型的可信性.分析结果表明,基于模糊集合的信任评估方法能够有效评估可信计算信任模型的可信性,丰富了可信计算信任评估理论.

8. 期刊论文 [罗芳, 徐宁, 周雁舟, 刘雪峰, Luo Fang, Xu Ning, Zhou Yanzhou, Liu Xuefeng](#) [可信计算中对象访问授权](#)

[协议的分析与改进](#) -[计算机应用与软件](#)2008, 25 (12)

可信平台模块的对象访问授权协议是可信平台模块安全的基础.依据可信计算对象访问授权模型,在对OIAP和IOSAP协议的特点及所存在的安全漏洞进行分析的基础上,提出了一个改进的对象访问授权协议.通过对改进协议的形式化分析和模拟实现,证明该协议可以抵抗外部调用者的替换攻击和中间人攻击.此外,通过在协议中引入对称密码算法,有效地解决了外部调用者和TPM之间授权认证和传输会话的机密性保护问题,在一定程度上提高了作为TCB信任根的TPM模块的安全性.

9. 学位论文 [周涛](#) [基于可信计算的Java智能卡虚拟机设计与实现](#) 2008

Java智能卡技术和可信计算技术是当前信息安全领域中的两个主要研究方向.一方面,Java智能卡以其特有的多应用性,越来越受到业界的重视,并得以广泛应用.与此同时,Java智能卡的多应用性也引发了相应的安全问题.目前已经出现了多种针对Java智能卡计算环境的攻击手段,这些不安全因素在一定程度上妨碍了Java智能卡的进一步普及和应用.

另一方面,为了增强现有PC终端体系结构的安全性,于1999年成立的可信计算组织(Trusted Computing Group,简称TCG)也推出了其可信计算技术规范,其目的是通过建立信任根和可信度量机制,力争在现有的,不可信PC环境中建立起可信的计算环境.但由于当前缺少基于可信计算技术的操作系统,因此,当前可信计算技术在实际应用中同样面临着一些难以解决的技术问题.

本论文在对这两种技术进行分析和研究的基础上,探索性地提出向Java智能卡虚拟机中引入可信计算技术,以提高Java智能卡计算环境安全性的设想,并以此为基础设计和开发了一套基于可信计算技术的Java智能卡卡内虚拟机.

10. 期刊论文 [胡浩, 张敏, 冯登国, HU Hao, ZHANG Min, FENG Deng-Guo](#) [基于信息流的可信操作系统度量架构](#) -[中国科学院研究生院学报](#)2009, 26 (4)

将信息流和可信计算技术结合,可以更好地保护操作系统完整性.但现有的可信计算度量机制存在动态性和效率方面的不足,而描述信息流的Biba完整性模型在应用时又存在单调性缺陷.本文将两者结合起来,基于Biba模型,以可信计算平台模块TPM为硬件信任根,引入信息流完整性,并提出了可信操作系统度量架构:BIFI.实验表明,BIFI不仅能很好地保护信息流完整性,而且对现有系统的改动很少,保证了效率.

[引证文献\(1条\)](#)

1. [曾颖明, 谢小权](#) [基于UEFI的可信Tiano设计与研究](#)[期刊论文]-[计算机工程与设计](#) 2009 (11)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_jsjgcysj200809015.aspx

下载时间: 2009年12月21日