信息安全理论与技术系列丛书

丛书主编：冯登国

国家自然科学基金重大研究计划项目（项目编号：91118006）
国家重点基础研究发展规划项目（项目编号：2013CB338003）

可信计算——理论与实践

冯登国　等 著

清华大学出版社

信息安全理论与

丛书主编：冯登国

可信计算——理论与实践

冯登国　等 著

清华大学出版社
北京

内 容 简 介

本书主要介绍可信计算技术的研究背景、发展现状、关键核心技术和应用技术，内容包括 TPM、TCM 和移动模块等可信平台模块，信任根、静态信任链构建系统、动态信任链构建系统和虚拟平台信任链等信任链构建技术，TSS、TSM 和可信应用开发等可信软件栈技术，可信 PC、可信服务器、可信移动平台、虚拟可信平台和可信计算平台应用等可信计算平台技术，可信平台模块测评、可信计算安全机制分析、可信计算评估与认证和可信计算平台综合测试分析系统等可信计算测评技术以及远程证明技术和可信网络连接 TNC。

本书可作为计算机、通信、信息安全、密码学等专业的博士生、硕士生和本科生教材，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目（CIP）数据

可信计算：理论与实践/冯登国等著. --北京：清华大学出版社，2013.5
信息安全理论与技术系列丛书
ISBN 978-7-302-31422-6

Ⅰ. ①可… Ⅱ. ①冯… Ⅲ. ①电子计算机－安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2013)第 018540 号

责任编辑：张　玥　战晓雷
封面设计：傅瑞学
责任校对：时翠兰
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.5　　**字　　数**：350 千字
版　　次：2013 年 5 月第 1 版　　**印　　次**：2013 年 5 月第1 次印刷
印　　数：1～2000
定　　价：29.50 元

产品编号：050513-01

丛书序

信息安全已成为国家安全的重要组成部分，也是保障信息社会和信息技术可持续发展的核心基础。信息技术的迅猛发展和深度应用必将带来更多难以解决的信息安全问题，只有掌握了信息安全的科学发展规律，才有可能解决人类社会遇到的各种信息安全问题。但科学规律的掌握非一朝一夕之功，治水、训火、利用核能曾经都经历了漫长的岁月。

无数事实证明，人类是有能力发现规律和认识真理的。今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋于真理的发展过程。信息安全是动态发展的，只有相对安全没有绝对安全，任何人都不能宣称自己对信息安全的认识达到终极。国内外学者已出版了大量的信息安全著作，我和我所领导的团队近 10 年来也出版了一批信息安全著作，目的是不断提升对信息安全的认识水平。我相信有了这些基础和积累，一定能够推出更高质量和更高认识水平的信息安全著作，也必将为推动我国信息安全理论与技术的创新研究做出实质性贡献。

本丛书的目标是推出系列具有特色和创新的信息安全理论与技术著作，我们的原则是成熟一本出版一本，不求数量，只求质量。希望每一本书都能提升读者对相关领域的认识水平，也希望每一本书都能成为经典范本。

我非常感谢清华大学出版社给我们提供了这样一个大舞台，使我们能够实施我们的计划和理想，我也特别感谢清华大学出版社张民老师的支持和帮助。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

冯登国

2009 年夏于北京

冯登国，中国科学院软件所研究员，博士生导师，教育部高等学校信息安全类专业教学指导委员会副主任委员，国家信息化专家咨询委员会专家，国家 863 计划信息安全技术主题专家组组长，信息安全国家重点实验室主任，国家计算机网络入侵防范中心主任。

前言

随着计算机网络的深度应用，最突出的三大安全威胁是恶意代码攻击、信息非法窃取、数据和系统非法破坏，其中，以用户私密信息为目标的恶意代码攻击超过传统病毒成为最大的安全威胁。这些安全威胁根源在于没有从体系架构上建立计算机的恶意代码攻击免疫机制，因此，如何从体系架构上建立恶意代码攻击免疫机制，实现计算系统平台安全、可信赖地运行，已经成为亟待解决的核心问题。

可信计算就是在此背景下提出的一种技术理念，它通过建立一种特定的完整性度量机制，使计算平台运行时具备分辨可信程序代码与不可信程序代码的能力，从而对不可信的程序代码建立有效的防治方法和措施。

我领导的可信计算研究团队从2003年便开始可信计算的研究工作。自2006年起我担任了中国可信计算工作组组长，一直在积极推动中国可信计算技术的研究、应用与产业化，取得了一定的成绩。我们可信计算研究团队先后承担了多项国家级项目，包括国家863计划项目、国家发改委高技术产业化项目和国家自然科学基金重大项目等，突破了信任链构建与修复技术、基于TCM安全芯片的远程证明协议、基于规约的测试用例自动生成方法等关键技术，成功研制了具有自主知识产权、技术先进的可信计算安全支撑平台，形成了支持标准符合性、安全性和实现特性的自主可信计算平台测评系统，取得了良好的经济效益和社会效益。我们的研究成果“可信计算安全支撑平台及其关键技术研究与应用”获得了2010年中国电子学会信息科学技术奖一等奖。我们将会继续奋斗下去，争取取得更多的优秀成果并获得更大的荣誉。

本书共8章。第1章是绪论，重点介绍可信计算的研究背景、技术发展现状和我们的主要贡献。第2章重点介绍可信平台模块，包括TPM、TCM和移动模块等。第3章重点介绍信任链构建技术，包括信任根、静态信任链构建系统、动态信任链构建系统和虚拟平台信任链等。第4章重点介绍可信软件栈，包括TSS、TSM和可信应用开发等。第5章重点介绍可信计算平台，包括PC、服务器、可信移动平台、虚拟可信平台和可信计算平台应用等。第6章重点介绍可信计算测评，包括可信平台模块测评、可信计算安全机制分析、可信计算评估与认证、可信计算平台综合测试分析系统等。第7章重点介绍远程证明技术。第8章重点介绍可信网络连接(TNC)。

参加本书写作的人员有秦宇博士、初晓博博士、徐静研究员以及博士生常德显、赵世军、邵建雄，在此对他们表示衷心的感谢。

本书在写作过程中得到了清华大学出版社的大力支持，以及国家自然科学基金重大研究计划项目(项目编号：91118006)和国家重点基础研究发展规划项目(项目编号：2013CB338003)的资助，也得到了张阳、张立武、张敏、孙锐、李昊等很多学者的帮助和支持，在此对他们表示衷心的感谢。

冯登国

2012 年 9 月于北京

目 录

第1章 绪 论

随着云计算、物联网和移动互联网等新型技术的快速发展，信息技术已经深刻地影响到社会的管理方式和人们的生活方式，无处不在的信息已经成为国家、企业和个人的重要资产。随着病毒和恶意软件等的泛滥，黑客攻击技术和能力的增强，这些重要信息资产将暴露在越来越多的威胁中。毫无疑问，提供一个可信赖的计算环境，保障信息的机密性、完整性、真实性和可靠性，已经成为国家、企业和个人最优先考虑的安全需求。传统的防火墙、入侵检测和病毒防御等网络安全防护手段都侧重于保护服务器的信息安全，而相对脆弱的终端就越来越成为信息系统安全的主要薄弱环节。针对这些系统安全需求和各类攻击手段，可信计算从计算机体系结构着手，从硬件安全出发建立一种信任传递体系以保证终端的可信，从源头上解决人与程序、人与机器以及人与人之间的信任问题。

可信计算就是在这种背景下应运而生的。对于“可信”这一概念目前有着众多不同的理解，为明确可信的含义，ISO/IEC、IEEE 和 TCG(Trusted Computing Group)等组织都给出了可信的准确定义[1-3]。TCG 组织在其可信定义理念下提出了通过嵌入在硬件平台上的可信平台模块(Trusted Platform Module，TPM)来提高计算机系统安全性的技术思路，得到了产业界的普遍认同。我们的思路与 TCG 类似，认为可信是指以安全芯片为基础建立可信的计算环境，确保系统实体按照预期的行为执行。

早在 20 世纪 90 年代中期，国外一些计算机厂商就开始提出可信计算技术方案，通过在硬件层嵌入一个安全模块，基于密码技术建立可信根、安全存储和信任链机制，实现可信计算安全目标。该技术思路于 1999 年逐步被 IT 产业界接受和认可，并形成可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)。同时，于 2001 年提出了 TPM 1.1 技术标准。之后，一些国际 IT 技术主导厂商推出了相关可信计算产品，得到用户和产业界的普遍认可。到 2003 年，TCPA 已发展成员近 200 个，几乎包括所有的国际 IT 主流厂商，随后改组为 TCG，并逐步建立起 TCG TPM 1.2 技术规范体系，其触角延伸到 IT 技术的每个领域。2009 年该规范体系的 4 个核心标准成为 ISO 标准。在产业发展上，Intel、微软公司在其核心产品中装配可信计算技术，到 2010 年，TPM 基本成为笔记本和台式机的标配部件。

我国在可信计算领域的重要贡献是打造了中国信息安全的 DNA——TCM 品牌，基于自主密码算法建立起了以 TCM 为核心的自主可信计算标准体系。我国可信计算的发展可划分为 3 个阶段。

第一个阶段为 2001—2005 年，是跟踪研究可信计算工作组(TCG)的技术理念的阶段。联想、兆日公司基于 TCG 技术体系开发出了相关产品。全国信息安全标准化技术委员会(TC260)WG1 工作组成立了可信计算标准工作小组，努力推进可信计算标准的研究。

第二个阶段为 2006—2007 年，是建立自主技术理论和标准体系的阶段。我国开展了基于中国密码算法的可信计算技术方案的研究，提出了《可信计算密码应用方案》，之后组建了可信计算密码应用技术体系研究专项工作组，后更名为中国可信计算工作组(China TCM Union，TCMU)，制订了以可信密码模块(Trusted Cryptography Module，TCM)为核心的

《可信计算密码支撑平台技术规范》[4]，并于2007年12月颁布了《可信计算密码支撑平台功能与接口技术规范》。

第三个阶段为2008年以后，是推动产业发展的阶段。在该阶段，TCM产品开始规模上市，并获得政府、军工和国计民生领域用户的高度认可。中国可信计算工作组目前有联想、同方和国民技术等29个成员单位，在政府的支持下，他们大力推进中国可信计算产业的发展。到2010年，在TCMU全体成员的共同努力下，我国已初步建立起由可信计算芯片、可信计算机、可信网络和应用、可信计算产品测评组成的产业体系。2008年中国信息协会信息安全专业委员会成立了可信计算联盟(China Trusted Computing Union，CTCU)，以推进可信计算的产业化。

1.1 国内外研究现状

可信计算的宗旨是以可信计算安全芯片为核心改进现有平台体系结构，增强通用计算平台和网络的可信性。国际可信计算组织TCG在现有体系结构上引入硬件安全芯片TPM，利用TPM的安全特性来保证通用计算平台的可信[5]。微软公司也发起了NGSCB[6]可信计算研究计划，采用微内核机制建立可信执行环境，为Windows平台安全和隐私保护提供支撑。与此同时，Intel公司也着力研究TXT硬件安全技术[7]，在微处理器、芯片组和I/O系统等硬件层面上支持可信计算。我国已成功研制出自主安全芯片TCM，并以此为基础建立了可信计算密码支撑平台体系结构。

近年来在产业界的推动下，可信计算得到了快速发展。而在学术界，国内外研究者也对可信计算技术进行了深入研究，在平台信任、网络信任和可信计算测评等方面取得了重要研究成果。其主要研究思路是：首先基于安全芯片建立终端平台信任，然后通过远程证明建立平台间的信任，最后将信任延伸到网络。

1.1.1 安全芯片研究现状

目前，国际主流的可信计算技术与规范体系由TCG提出，其历史最早可追溯至20世纪90年代。作为可信计算技术的核心，TPM安全芯片规范于2001年提出，并被多次修改。TPM的主要作用是作为计算平台的信任根基，提供受保护的关键密码学功能和存储空间，进而同其他软硬件技术一起构建可靠的计算平台。目前，TPM规范已经被几乎所有IT业界巨头所认可和接纳，TPM实体芯片已经广泛配备于各类笔记本、个人计算机、服务器和其他类型的计算平台，成为多种可信服务与应用的核心部件。

我国可信计算标准于2007年提出，符合该标准的TCM安全芯片随之陆续上市。TCM从总体上借鉴了国际可信计算技术框架与技术理念，但具体的设计和思路与TPM存在较大的不同，这主要体现在更加安全、高效的椭圆曲线密码学算法，以及针对我国具体安全与市场需求所进行的若干关键技术创新。

近年来，安全芯片的技术发展呈现出一些重要的新态势。2006年，TCG的移动平台工作组首次颁布了移动可信模块规范。与TPM和TCM相比，移动可信模块的实现与部署形式更加灵活，所覆盖的利益相关方更加全面，体现出安全芯片对新式平台及可定制性、可验证性和可升级性的高度重视。另外，国际信息产业巨头还陆续推出一批系统安全技术，包括

Intel TXT 和 ARM TrustZone 等。这些技术与可信安全芯片密切相关，从构建可信执行环境的角度已经形成了互相配合、互为补充的全新技术体系。

1.1.2 终端平台信任技术研究现状

建立终端平台信任的主要技术手段是信任链的构建。从构建的时间讲，信任链构建可分为可信引导与操作系统度量两个阶段；从构建的方式讲，信任链构建又可分为静态和动态两类。截至目前，信任链构建的主要工作集中于操作系统度量方面。早期的代表性信任链系统是借助外设进行度量的 Copilot 系统[8]和 Pioneer 系统[9]。TCG 提出以 TPM 为信任根，适用于通用终端平台的构建度量系统的方法。在 TCG 框架下，IBM 公司 T. J. Watson 研究院率先提出了完整性度量架构 IMA[10]，并又推出了改进架构 PRIMA[11]。卡内基·梅隆大学在此框架下提出了适用于分布式环境的细粒度度量架构 BIND[12]。我国学者在此基础上也提出了一些可行的解决方案[13,14]。

终端平台信任的另一个研究领域是可信软件栈。可信软件栈可以看作是硬件层的可信安全芯片功能向应用层的包装与延伸，是可信计算平台内部最重要的软件组件之一。TCG 已经发布了可信软件栈的相关规范，详细定义了该类软件应当遵循的架构与接口设计。2005 年，IBM 公司最先发布了遵循上述规范的 Trousers 软件栈，成为可信计算方面奠基性的开源软件产品之一。针对 Java 和移动平台的具体需求，奥地利格拉兹大学的 IAIK 研究所和德国的 Sirrix AG 公司还分别开发了 jTSS 和 uTSS 两种新型的可信软件栈。

基于上述技术，产业界和学术界陆续推出了采用可信计算机的个人计算机和服务器等产品。近年来，随着新技术和新需求的发展与变化，两类新型的终端计算平台得到了越来越多的关注。可信移动平台方面，研究者借鉴移动可信模块的基本设计思想，基于多种硬件形态与技术实现了具有可信计算功能和特性的终端平台。这方面最主要的成果是奥地利格拉兹大学的 IAIK 研究所研制的基于 Java 卡和 ARM TrustZone 技术设计与实现的原型系统。虚拟平台方面，研究者充分运用了虚拟技术的隔离特性，从保护核心程序不受干扰的思想出发，给出了一大批先进的技术方案，主要成果包括 LKIM 系统[15]、HIMA[16]和 HyperSentry 度量架构[17]。LKIM 和 HIMA 都是利用虚拟平台的隔离特性，通过对虚拟机内存的监控实现对虚拟机的完整性度量。而 HyperSentry 采用硬件机制，在 Hypervisor 无法感知的情况下对其进行度量。虚拟平台构建信任的基础在于建立为多个虚拟机提供信任服务的信任根。IBM 公司提出了 vTPM 架构[18]，以软件虚拟的方式为每个虚拟机提供一个单独的 vTPM，从而规避多个虚拟机共享 TPM 的资源冲突问题。德国波鸿鲁尔大学在 vTPM 架构的基础上提出了基于属性的 TPM 虚拟方案[19]，进一步增强了 vTPM 的可用性。这两种方案的不足都在于 vTPM 与 TPM 之间缺乏有效绑定。

1.1.3 平台间信任扩展技术研究现状

在终端平台信任构建的基础上，将终端平台的信任扩展到远程平台的主要方法是远程证明，它主要包括平台身份证明和平台状态证明。

在平台身份证明方面，TPM v1.1 规范首先提出了基于 Privacy CA 的身份证明方案，它通过平台身份证书证明平台真实身份，该方案无法实现平台身份的匿名性。针对 TPM 匿名证明的需求，TPM v1.2 规范提出了基于 CL 签名[20]的直接匿名证明(Direct Anonymous

Attestation,DAA)方案[21]。随后,He 等学者针对嵌入式设备的特点,提出了一种效率更高的改进的 DAA 方案[22]。DAA 的早期研究主要针对 RSA 密码体制展开,这方面的研究都存在 DAA 签名长度较长、计算量大的缺点。Brickel 等学者采用 LRSW 假设[23]提出了首个基于椭圆曲线及双线性映射的 DAA 方案[24],大幅度提高了计算和通信性能。随后,我们基于 q-SDH 假设[25]对 DAA 方案进行了深入研究,进一步提高了计算和通信效率[26]。近年来,Brickell 和 Chen 等学者采用新的密码学假设对 DAA 进行了深入的研究,显著优化了 TPM 的协议计算量[27,28],并且利用 ARM 处理器进行了模拟分析[29]。

在平台状态证明方面,TCG 提出二进制直接远程证明方法,IBM 公司遵循该方法实现直接证明的原型系统[30]。这种方法存在平台配置容易泄漏、扩展性差等问题。为克服上述弊端,国际上提出了基于属性的证明方法,将平台配置度量值转换为特定的安全属性,并加以证明。这方面的主要研究成果有 IBM 公司基于属性证明的框架[31]和德国波鸿鲁尔大学的属性远程证明实现方案[32]。随后,Chen 等学者提出了一个具体的基于属性的远程证明协议[33],该协议支持盲验证和属性的撤销,并在随机预言模型下可证明其安全性。随着属性证明的深入研究,Ulrich 等学者提出了一种具体属性证明实现方法[34],它无须修改现有的硬件与软件架构。针对无第三方可用的特殊场景,Chen 等学者采用环签名方法给出了基于无须可信第三方的基于属性的远程证明协议[35]。利用 TPM 对配置-属性的承诺构建环签名密钥,将具体配置情况隐藏在特定的属性集合当中。此外,Haldar 等学者提出了基于语义的证明[36],利用可信虚拟机向远程方证明 Java 高级语言程序的语义安全。卡内基·梅隆大学针对特殊的嵌入式设备提出了基于软件的证明[37]。我国学者将平台配置状态转化为平台历史行为序列,提出了基于系统行为的证明[38]。

1.1.4 可信网络研究现状

随着网络应用的普及,仅有终端可信是不能满足需求的,还需将终端的信任扩展到网络,将网络构建成一个可信的计算环境。

在可信网络接入控制方面,思科公司和微软公司分别推出了网络接入控制(NAC)方案[39]和网络访问保护(NAP)方案[40]。NAC 的优势在于网络设备的接入控制和监控,NAP 的优势在于终端安全状态评估和监控。TCG 于 2005 年发布了可信网络连接(Trusted Network Connection,TNC)架构规范 1.0 版本[41],其特点在于将终端完整性引入网络接入控制的判定当中。TCG 对网络接入规范进行了持续的改进,在最新发布的规范中,TNC 架构增加了元数据存取点(Meta Access Point,MAP)和 MAP 客户端,能够根据元数据信息的变化动态控制终端对网络的访问,同时 TNC 架构还实现了与 NAP 方案的互操作。我国学者基于 TNC 架构也开展了可信网络连接的研究工作[42]。

现有的网络安全协议,如 SSL/TLS 协议和 IPSec 协议,只能实现终端接入可信网络时的用户身份认证,保证网络通信数据的机密性和完整性,无法实现终端完整性的认证。针对该问题,IBM 研究院提出了将终端完整性证明扩展到 SSL 协议的方案[43],终端通过与可信网络协商安全参数并在 SSL 协议上证明平台配置状态,以此建立终端与可信网络之间的可信信道。然而,这种简单的扩展方案容易遭受中间人攻击。德国波鸿鲁尔大学在可信虚拟平台上提供平台属性证书,将 SSL 身份和 AIK(Attestation Identity Key)身份绑定解决上述问题[44],为了更好地兼容 TLS 规范,进一步给出了基于 OpenSSL 建立可信信道的实现

方法[45]。

1.1.5 可信计算测评研究现状

在可信计算测评方面，具体的研究方向可大致分为可信平台模块合规性测试、安全机制分析和可信计算产品评估认证3类。

顾名思义，可信平台模块合规性测试是指测试可信平台模块与相关规范的符合程度。它是可信计算测评领域最重要的研究方向之一。在这一方面，德国波鸿鲁尔大学给出了第一个针对TPM的解决方案[46]，该方案描述了手工测试TPM的详细步骤。其不足是自动化程度较低，也无法分析测试结果质量。中国人民大学和武汉大学研究了TPM合规性测试的自动化问题，提出了新型的随机测试用例生成方法[47,48]。以TPM/TCM扩展有限自动机测试模型为基础，中国科学院软件研究所提出了包括可信平台模块测试模型、测试用例自动化生成方法和测试用例质量分析的系统化合规性测试方法，并在实际测试工作中取得了良好效果[49,50]。

可信计算安全机制分析是传统的安全协议分析研究在可信计算领域的体现。该类研究的主要对象是可信计算领域中较为抽象的协议与关键运行机制，例如TPM/TCM的授权协议、DAA协议、PCR扩展机制和可信计算平台的信任链构建机制等。可信计算安全机制分析的目标是在理论层面发现分析对象的安全隐患或证明分析对象的安全性质。因此，这部分研究一般采用形式化分析方法，这些方法大致可归为模型检验和定理证明两大类。目前，意大利米兰大学、德国波鸿鲁尔大学、美国卡内基·梅隆大学和中国科学院软件研究所等，已经陆续发现了TPM的授权协议[51,52]、TCM授权协议[53]、DAA协议[54]、信任链建立[55]和迁移机制[56]等协议与关键机制中存在的安全隐患。

可信计算产品评估源于国际信息安全领域对安全工程思想的逐渐重视。根据该思想，为保障产品的安全性，需要对产品需求设定、设计、生产和部署的全过程加以控制和评估。目前，TCG启动了针对TPM芯片[57]和可信网络连接产品的评估项目，并已经取得了一定成果：Infineon公司的TPM SLB9635TT1.2成为通过依据TPM保护轮廓[58]评估的首款芯片[59]，而美国的Juniper网络公司(Juniper Technologies)和德国汉诺威应用技术大学(Hochschule Hannover)等的IC4500综合访问控制套件、EX4200交换机和StrongSwan等7款TNC相关产品得到了TCG认证。

综上所述，目前可信计算测评方面的研究成果数量相对较少，完备和深入程度都有待提高。第一，从测评目标来看，现有方法仅能验证与分析一小部分可信计算产品与安全机制，对下文介绍的一些最新可信计算相关技术尚无能为力；第二，从测评的层次来看，现有方法停留在组件级别，复杂的系统级测评研究基本处于空白状态；第三，从测评所依据的标准来看，只有安全芯片等个别产品同时具备功能规范和测试规范，大部分可信计算产品与机制没有测试规范进行指导，甚至有一些安全机制(例如信任链)连详细的功能规范都无从依据。

1.2 我们的主要工作

从2003年起，本书作者领导的研究团队对可信计算关键技术进行了系统深入研究，主要贡献可归纳为以下几个方面。

(1) 可信计算信任模型及信任构建方面,针对原有完整性度量架构缺乏动态性、扩展性等问题,建立了基于信任度的信任模型,提出了可恢复的可信引导系统建立方法和操作系统动态度量方法,并在上述方法的基础上实现了从系统引导到应用程序运行的完整信任链系统。

(2) 远程证明方面,构造了首个双线性对属性远程证明方案,以及首个基于 q-SDH 假设的双线性对直接匿名证明方案,这些重要成果提升了我国远程证明协议的研究水平。采用双线性对的方法拓宽了远程证明协议的研究思路,为促进远程证明关键技术实际应用奠定了理论基础。

(3) 可信计算测评方面,基于扩展的有限自动状态机模型,提出了一种基于规约的测试用例自动生成方法;采用该方法研制实现了支持 TPM/TCM 安全芯片合规性测试等功能的可信计算平台测评系统,目前该测评系统已经应用于国内权威测评机构;对 TCM 安全芯片的授权协议进行了形式化分析,发现了针对该协议的重放攻击。这些测评研究成果对于提高可信计算产品安全性、改进产品质量和规范产业发展起到了重要作用。

1.2.1 可信终端信任构建

可信终端信任构建是建立平台信任和网络信任的基础,也是当前可信计算研究的热点问题。在信任模型方面,我们综合考虑终端启动时各组件对信任的影响,建立了基于信任度的终端信任模型。在信任链构建方法方面,我们分别针对系统引导阶段和操作系统运行阶段提出了效率高、安全性好的度量方法,整体构成了一条从终端启动到应用程序运行的完整信任链。

1. 基于信任度的信任模型

构建终端平台的信任必须建立信任模型,以保证平台所有实体启动时和运行时的可信。TCG 以安全芯片为信任根,通过逐级认证实体完整性的方式,建立平台启动时信任,然后利用 BLP、Biba 等访问控制模型建立平台运行时信任。然而,这种启动时实体信任建立方式未考虑平台运行环境,而实体的可信启动可能受之前已运行实体的影响;这种基于访问控制模型的运行时信任建立方式缺乏信任程度及其变化的判定依据,存在实施困难、可用性差等问题。为此,我们研究提出了基于信任度的信任模型[60,61],利用信任度的概念综合考虑平台启动时已运行实体对启动实体的影响,建立平台启动时的信任,同时给出了在平台运行时动态调节实体信任度的信任规则,并基于实体的信任度实施访问控制,建立平台运行时的信任。

2. 可恢复的可信引导信任链构建方法

针对计算平台在可信引导过程中信任链遭受破坏后不易恢复的问题,我们提出了一种可恢复的可信引导信任链构建方法。主要思想是首先建立系统启动到操作系统引导前的信任链,并对其进行验证,然后检查操作系统内核镜像以及关键文件的完整性,如果检查失败则进入一个安全系统对系统进行修复。

基于上述方法我们实现了一个可信引导子系统,其以 TPM/TCM 为信任根,在正常的系统引导功能基础上扩展了系统部件的度量和验证、引导流程的配置、信任链构建及恢复等功能。当可信引导子系统能够启动时,TPM/TCM 依次度量操作系统运行前的各阶段组