计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(8): 1332-1349, 2011

可信计算技术研究

冯登国 秦 宇 汪 丹 初晓博
(信息安全国家重点实验室(中国科学院软件研究所) 北京 100190)
(feng@is.iscas.ac.cn)

Research on Trusted Computing Technology

Feng Dengguo, Qin Yu, Wang Dan, and Chu Xiaobo
(*State Key Laboratory of Information Security* (*Institute of Software*, *Chinese Academy of Sciences*), *Beijing* 100190)

Abstract Trusted computing, as a novel technology of information security, has become an important research area of information security. TCG comprised of the international IT giants has published a series of trusted computing specifications to promote the comprehensive development of the trusted computing technology and industry, and the core specifications have been accepted as international standardization by ISO/IEC. In academia, the research institutions at home and abroad study the trusted computing technology in depth and have gained rich achievements. In China, the independent trusted computing standard infrastructure is founded with the core of TCM on the basis of the independent cryptography algorithms, forming the whole trusted computing industry chains, which breaks the monopolization of the trusted computing technology and industry by the international IT giants. With the rapid development of trusted computing field, there are still lots of problems on the key technologies to be solved, and the related research has been done in succession recently. This paper comprehensively illustrates our research results on trusted computing technology. Beginning with establishing the trust of the terminal platforms, we propose a trustworthiness-based trust model and give a method of building trust chain dynamically with information flow, which ensure the real time and security protection of the trust establishment to some extent. Aiming at the security and efficiency problems of the remote attestation protocols, we propose the first property-based attestation scheme on bilinear map and the first direct anonymous attestation scheme based on the q-SDH assumption from the bilinear maps. In trusted computing testing and evaluation, we propose a method of generating test cases automatically with EFSM, and from the method develop a trusted computing platform testing and evaluation system which is the first to be applied in China practically.

Key words trusted computing; TPM; TCM; trust chain; remote attestation; trusted computing testing and evaluation

摘 要 可信计算技术作为一种新型信息安全技术,已经成为信息安全领域的研究热点.在可信计算领域取得长足发展的同时,其关键技术仍存在许多问题亟待解决,近年来这方面的相关研究已经陆续展开.综述了在可信计算关键技术方面的研究成果,从构建可信终端的信任入手,建立了基于信任度的信任模型,给出了基于信息流的动态信任链构建方法,一定程度上解决了终端信任构建的实时性、安全性等问题.针对远程证明协议的安全性和效率问题,构造了首个双线性对属性远程证明方案和首个基于

收稿日期:2011-04-07;修回日期:2011-06-24
基金项目:国家"九七三"重点基础研究发展计划基金项目(2007CB311202)
通信作者:汪 丹(wangdan@is.iscas.ac.cn)

q-SDH 假设的双线性对直接匿名证明方案.在可信计算测评方面,提出了一种基于扩展有限状态机的测试用例自动生成方法,并基于该方法研制了国内首个实际应用的可信计算平台测评系统.

关键词 可信计算;可信平台模块;可信密码模块;信任链;远程证明;可信计算测评

中图法分类号 TP309

随着计算机网络的深度应用,最突出的首 3 位安全威胁是[1]: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.

目前可信计算中的可信存在多种不同定义.ISO/IEC 将可信定义为[2]:参与计算的组件、操作或过程在任意的条件下是可预测的,并能够抵御病毒和一定程度的物理干扰.IEEE 给出的可信定义为[3]:计算机系统所提供服务的可信赖性是可论证的.TCG(Trusted Computing Group)将可信定义为[4]:一个实体是可信的,如果它的行为总是以预期的方式,朝着预期的目标.TCG 的可信计算技术思路是通过在硬件平台上引入可信平台模块 TPM(trusted platform module)来提高计算机系统的安全性,这种技术思路目前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 TPM1.1 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,至此可信计算成为 IT 产业发展趋势.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 TCPA 改名为 TCG,并逐步建立起 TCG TPM1.2 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 国际标准.在产业发展上,Intel、微软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.

我国一直高度重视可信计算技术,承载着核心技术自主创新、信息安全自主掌控的信念,大致经历了 3 个发展阶段:

第 1 个阶段为 2001 年至 2005 年,是消化吸收 TCG 技术理念阶段.联想、兆日基于 TCG 技术体系开发出相关产品,瑞达也提出了一套 PC 安全技术路线.全国信息安全标准化技术委员会(TC260)成立了可信计算标准工作小组,推进中国可信计算标准的研究.

第 2 个阶段为 2006 年至 2007 年,建立自主技术理论和标准体系阶段.我国有关管理部门意识到可信计算给中国 IT 产业自主创新带来发展机遇,专门组织学术界和企事业单位,开展基于中国密码算法的可信计算技术方案研究,提出《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(后改名为中国可信计算工作组(China TCM Union,TCMU),联想、国民技术、中国科学院软件所、同方、兆日、瑞达等 11 家单位加入该工作组,制定出以 TCM(trusted cryptography module)为核心的《可信计算密码支撑平台技术规范》系列标准[5],并于 2007 年 12 月颁布《可信计算密码支撑平台功能与接口技术规范》,同时,国民技术、联想、同方、方正、长城、瑞达等均开发出基于此标准的产品.

第 3 个阶段为 2008 年以后,推动产业发展阶段.TCM 产品开始规模上市,获得政府、军工、国计民生领域用户高度认可.中国可信计算工作组目前有国民技术、联想、同方、中国科学院软件所、方正、卫士通等 29 个成员单位,由企业牵头,政府支持,大力推进中国可信计算产业的发展.到 2010 年,在 TCMU 全体成员共同努力下,已建立起可信计算芯片、可信计算机、可信网络和应用、可信计算产品测评

的基本完整的产业体系.

中国科学院软件所作为 TCMU 的核心成员,重点开展可信计算关键技术研究,目前已经取得了多项创新成果,这些成果正在自主可信计算产业中得到推广应用.具体研究思路是:从安全芯片的信任构建出发,按照信任构建范围,从小到大,依次研究构建终端信任、平台间信任、网络信任的关键技术,基于这些关键技术研究可信计算应用,提升现有应用解决方案的安全性,并进一步研究可信计算测评技术以规范可信计算产品的生产和认证.本文在分析国内外可信计算技术研究现状的基础上,系统地介绍了我们的研究成果.

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[6].微软也发起了 NGSCB[7] 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 也着力研究 TXT 硬件安全技术[8],在微处理器、芯片组、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 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完整性度量.在早期的度量系统中,具有代表性的是马里兰大学的 Copilot 系统[9] 和卡内基梅隆大学的 Pioneer 系统[10],它们分别借助专用 PCI 板卡和外部可信实体执行度量工作,它们的不足都是无法适用于通用终端平台.TCG 提出以 TPM 为信任根,逐级度量启动过程中的硬件、操作系统和应用程序的方法,以此建立通用终端平台的信任.IBM 研究院研发了最早的 TCG 框架下的完整性度量架构 IMA[11],其特点是在可执行文件装载时对其进行完整性度量,缺陷是对所有装载程序都进行度量,系统效率较低.对此他们又进一步提出了 PRIMA 度量架构[12],该架构将度量与信息流访问控制模型相结合,从而大幅度精简度量对象,提高系统效率.上述 2 种度量架构都只能静态度量可执行文件,无法保证程序在运行过程中可信.卡内基梅隆大学提出了 BIND 度量系统[13],其扩展了编程语言的度量语义,包含度量标记的代码被执行时会激活 BIND 系统对其完整性度量.BIND 系统在一定程度上实现了对软件关键代码动态行为的度量.但是需要软件开发者手动添加度量标记,编程要求较高.我国学者针对静态度量的不足也提出了一些解决方案[14-15].

随着虚拟技术的发展,终端平台的虚拟化应用越来越广泛,虚拟平台度量技术的研究逐渐成为研究热点.这方面的主要成果包括 LKIM 系统[16]、HIMA[17] 和 HyperSentry 度量架构[18].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 提出了 vTPM 架构[19],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[20],进一步增强 vTPM 的可用性.这 2 种方案的不足都在于 vTPM 与 TPM 之间缺乏有效绑定.

1.2 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[21] 的直接匿名证明 DAA(direct anonymous attestation)方案[22].随后,He Ge 等人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[23].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 等人采用 LRSW 假设[24] 提出了首个基于椭圆曲线及

双线性映射的 DAA 方案[25],大幅度提高计算和通信性能.随后,我们基于 q-SDH 假设[26]对 DAA 方案进行了改进研究,进一步提高了计算和通信效率[27].近年来,Chen Liqun 等人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[28-29],并且利用 ARM 处理器进行了模拟分析[30].

在平台状态证明方面,TCG 提出二进制直接远程证明方法,IBM 遵循该方法实现直接证明的原型系统[31].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 基于属性证明的框架[32]和德国波鸿鲁尔大学的属性远程证明实现方案[33].随后,Chen Liqun 等学者提出了一个具体的基于属性的远程证明协议[34],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,Kuhn 等人提出了一种具体属性证明实现方法[35],它无需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 Liqun 等人采用环签名方法给出了基于无需可信第三方的基于属性的远程证明协议[36].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 等人提出了基于语义的证明[37],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[38];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[39].

1.3 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.

目前,国际上已有一些研究机构启动了可信网络的研究计划.美国国防先进研究项目局提出了 CHAT 项目[40],探讨如何在对安全性、可靠性、可生存性及其他必要属性具有严格要求的条件下,得到可以验证的可信系统和网络.卡内基梅隆大学推出了 TRIAD 项目[41],研究如何借助入侵检测提高网络系统的可信性.我国学者在可信网络研究方面也取得了一定的成果,提出了可信网络的概念和相关模型,给出了网络可信属性的定量计算方法[42].

在可信网络接入控制方面,思科和微软分别推出了网络接入控制(NAC)方案[43]和网络访问保护(NAP)方案[44],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 组织于 2005 年发布了可信网络连接 TNC(trusted network connection)架构规范 1.0 版本[45],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 MAP(meta access point)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[46].

现有的网络安全协议,如 SSL 协议(或 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[47],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[48],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[49].

1.4 可信计算测评与分析研究现状

可信计算测评与分析方面的工作主要包括可信计算标准符合性测评和可信计算协议及系统安全性分析.

在可信计算标准符合性测评方面,德国波鸿鲁尔大学给出了第 1 个详细的 TPM 规范符合性测试方案和相应的测试结果[50].该方案自动化程度较低,也无法分析测试结果的覆盖度.我国学者在 TPM 的自动化测试方面进行了研究[51],并研究了 TPM 符合性测试用例自动生成问题,提出了一种改进的随机测试用例生成方法[52],同时从可信计算平台形式化模型入手,给出了一套完整的信任链测试方法.除了上述测试工作以外,可信计算评估工作也陆续展开.TCG 启动了针对 TPM 芯片和可信网络连接产品的评估项目[53],其中 Infineon 公司的 TPM SLB9635TT1.2 成为通过依据 TPM 保护轮廓[54]评估的首款芯片产品[55].

在可信计算协议及系统安全性分析方面,意大利

米兰大学使用 SPIN 工具对 TPM 授权会话协议进行了分析,发现了 OIAP 协议存在重放攻击的问题[56],攻击者可以重放已经执行过的命令从而回滚 TPM 状态.英国惠普公司使用 Murphi 有限状态自动机检测工具也对 TPM 授权会话协议进行了分析,分析结果显示该协议在共享授权秘密场景下易遭受 TPM 伪装攻击[57].德国萨尔大学利用 π 演算方法分析了 DAA 协议,发现了 DAA 协议的一个安全缺陷[58]:攻击者可以使得匿名凭证颁发者无法精确统计已持有证书的平台.美国卡耐基梅隆大学采用安全系统逻辑分析了 TPM 完整性收集和报告功能[59],发现攻击者可以任意修改平台 PCR(platform configuration register)值,破坏了基于动态度量信任根的信任传递机制.我们针对国产安全芯片 TCM 的部分关键机制进行了模型检验分析[60],其操作性更强,自动化程度更高.我国学者在 TCG 框架下给出了一个利用迁移机制窃取密钥信息的有效攻击方法[61].

总体而言,可信计算测评的研究与实践尚未完全成熟,一些关键测评技术亟待研究.在可信计算标准符合性测试方面,已有方法自动化程度较低,实施效率不高,也不能提供全面的测试结果分析.在可信计算评估方面,现有的评估方法的应用范围有限,其可用性还需实践检验.

2 我们的主要工作

我们近几年对可信计算关键技术进行了系统深入研究,在可信终端信任构建方面,给出了基于信任度的信任模型,同时从动态性、信息流等角度提出了终端信任链构建方法;在远程证明方面,重点从安全性和性能两方面改进了现有的直接匿名证明和属性证明协议;在可信网络连接方面,将可信网络接入和直接匿名证明相结合研究了平台匿名网络接入控制机制.在可信计算应用方面,从数据存储及使用安全的角度,提出了可信存储和可信使用控制应用解决方案.在可信计算测评方面,基于扩展的有限状态机提出了可信计算测评模型和自动化测试方法.

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.我们在信任模型和信任链方面开展了一些研究工作,主要包括基于信任度的终端平台信任模型、动态信任链构建方法,以及虚拟计算平台的信任链构建方法.

2.1.1 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保证平台所有实体启动时和运行时的可信.TCG 以 TPM 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.建立平台运行时信任目前最常用的方法是使用 BLP,Biba 等访问控制模型.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[62-63],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.

平台信任建立首先必须描述启动过程中 2 实体 A 与 B(A 触发启动 B)之间的信任关系,A 依据 B 的历史行为定义 B 启动时的信任度 $t_{A,B}=E[r_B \mid s_A h_B]$,式中 r 是实体的信誉,s 是平台状态,h 是实体的历史行为.信任度值的计算可以采用 Beta 信任度评估模型中的方法.然后,采用这种描述方式递归定义信任根 TPM/TCM 对实体 k 的信任度 $t_k=E[r_1 r_2 \cdots r_{k-1} r_k \mid s_{\mathrm{TPM}} h_1 h_2 \cdots h_{k-1} h_k]=t_{\mathrm{TPM},1}\, t_{1,2} \cdots t_{k-2,k-1} t_{k-1,k}$,继而可以定量描述平台各个启动阶段的信任.最后,基于实体信任度实施访问控制建立平台运行时信任,由于实体信任度在其访问操作完成后可能会发生变化,我们定义了信任度降低规则和信任度调节规则:1)信任度降低规则,主要适用于主体信任度高于客体信任度的情况,在访问操作完成后主体信任度应降为客体信任度;2)信任度调节规则,主要针对主体的变化,对主体实体进行重新认证确定其信任度.在整个信任模型中,信任度的计算、调整,以及基于信任度的访问控制,综合考虑了平台实体启动和运行时的安全影响因素,可用性更好.

2.1.2 动态信任链构建方法

信任链构建方法的核心是在信任链模型的基础上分别针对系统引导、操作系统、应用程序等各运行阶段提出效率高、安全性好的度量架构和信任链构建方法.我们主要在信任链的可恢复性和动态性方面进行了深入研究.

1) 可恢复的可信引导信任链构建

针对计算平台在可信引导过程中信任链容易遭受破坏的问题,我们设计并实现了一种可恢复的可信

引导信任链构建系统(称之为 LOIS Grub 系统),该系统可以灵活地支持认证引导和安全引导等多种引导模式,其核心功能是通过修复系统关键文件的方法实现操作系统信任链恢复.

LOIS Grub 系统以 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.当可信引导器 LOIS Grub 启动时,TPM/TCM 依次度量 Stage1,然后运行 Stage1,并由 Stage1 度量 Stage2.在 Stage2 阶段扩展信任链验证和恢复功能,对在此之前的信任链进行验证,并检查操作系统重要文件和内核的完整性,如果验证通过则正常引导操作系统,否则执行信任链的恢复.

LOIS Grub 系统大大提高了可信计算平台信任链在可信引导阶段的健壮性,而且信任链恢复功能对系统性能影响极小,所产生的系统启动延迟完全在用户可接受范围之内.

2) 操作系统阶段信任链构建方法

操作系统阶段信任链构建比可信引导阶段要复杂得多,要建立操作系统信任链必须设计和实现一种高效的度量架构.IBM 的 IMA 度量架构是传统操作系统信任链构建方法的代表,它存在度量实时性差、冗余度高,且易遭受 TOCTOU(time of check, time of use)攻击的问题.我们针对这些问题提出一种基于信息流的动态度量方法[64-65],该方法不仅能够对操作系统内核模块、进程进行动态度量,还能根据 Biba 的完整性信息流规则简化进程的度量.

根据上述思想我们设计并实现了一种基于信息流的操作系统动态度量架构 DIMA,如图 1 所示.其中,度量代理 MA(measurement agent)一部分处于用户空间,一部分位于内核空间,它负责接收用户的度量请求对系统进程进行动态度量.进程度量时 MA 必须首先调用 Biba-Invoke,根据强制访问控制策略检查信息流完整性符合情况后再实施度量.内核度量模块处于内核空间,专门对系统内核服务、驱动等内核模块实施动态度量.DIMA 度量架构自身的安全建立在可信引导阶段信任链基础上.

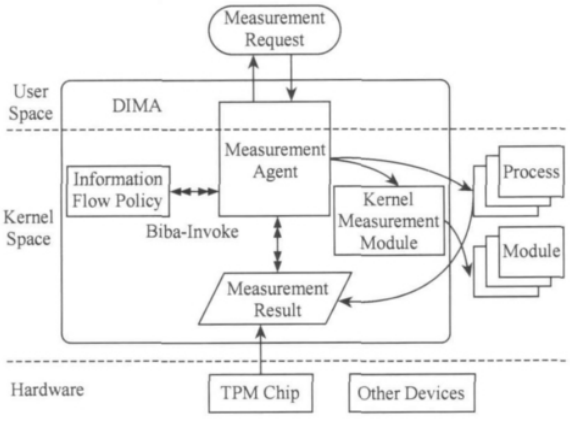

Fig. 1 DIMA measurement architecture.

图 1 DIMA 度量架构

根据度量对象的不同,DIMA 度量架构分 2 种情况实施信息流动态度量:1)进程度量.当度量请求发生时 MA 首先检查信息流完整性,如果违背强制访问控制策略,则拒绝进程执行,不进行任何度量.如果符合信息流策略,则首先动态度量进程在内存中的镜像,度量结果为 $H(P)$,然后再验证 $H(P)$是否符合策略要求.如果验证通过则调用 Biba-Invoke 获取进程主体 S、访问客体 O、实际操作 A 等信息,并形成最终的信息流动态度量结果 $m=H(S\|O\|A\|H(P))$;如果验证不通过,则拒绝该进程的执行.2)内核模块度量.由于只需要动态保证内核模块提供的服务是可信的,因此无需信息流度量.操作系统维护了一个内核模块链表,通过查询该链表获取内核模块的关键数据进行动态度量,以此保证它们的可信.

基于信息流的动态度量方法一定程度上实现了操作系统的动态度量,避免了 TOCTOU 攻击.并且我们基于 Linux 操作系统实现了 DIMA 度量架构,通过构建仿真攻击进行了安全性验证,实验结果表明 DIMA 能检测出常见的进程完整性篡改,而且对系统性能影响比较小.目前,这种将信息流和动态度量相结合的研究还是初步的,还有很多问题值得进一步深入研究.

2.1.3 虚拟平台信任链构建方法

随着虚拟化技术在终端平台的广泛应用,虚拟平台信任构建显得日趋重要.由于虚拟平台上多个虚拟机同时运行,其信任根的实现方式、信任链的构建方式与普通终端平台截然不同,存在多条动态变化的信任链.我们在借鉴 vTPM 思路的基础上,提出了一种虚拟平台信任链动态构建方法[66].该方法不再使用普通平台链式传递信任的方式,而是采用杂凑树和虚拟 PCR 的方式构建虚拟机动态信任链(如图 2 所示),并且还给出了完整性度量算法和信任链更新算法以实现虚拟平台信任链的扩展和更新.

这种方法克服了 TCG 的静态信任链的不足,支持信任链的动态更新,能够反映出虚拟平台信任链的最新状态.依据该方法我们在 Xen 虚拟化平台

上实现了原型系统,验证了该信任链构建方法的可行性和高效性.

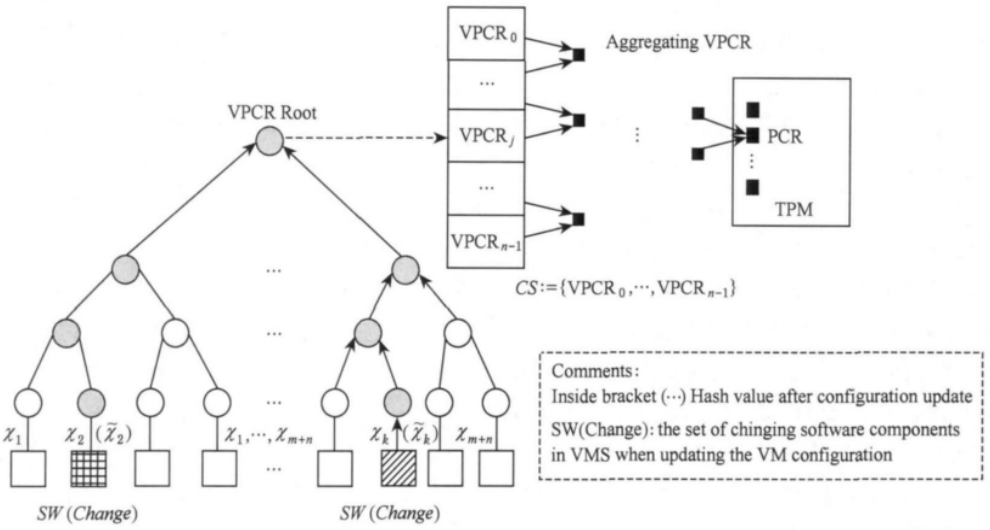

Fig. 2 Dynamic trust chain for virtual machine.

图 2 虚拟机动态信任链

2.2 远程证明

远程证明是可信计算用于解决可信计算平台之间、可信网络节点信任的重要安全机制. 远程证明包含平台身份的证明和平台完整性状态的证明,这 2 种证明的基本模型非常类似,包含一个带有 TPM/TCM 的可信计算平台 P、验证平台 V 和辅助支持验证的可信第三方 T. 远程证明基本模型的信任锚点是安全芯片 TPM/TCM,以及颁发平台证书(平台身份证书,或者平台属性证书)的可信第三方,安全芯片保证了平台的真实性,可信第三方确保了协议的正确性.

当前远程证明的研究热点是远程证明协议,主要研究方向是直接匿名证明协议(direct anonymous attestation,DAA)和基于属性证明协议(property-based attestation,PBA).

2.2.1 直接匿名证明

1) 下一代可信计算直接匿名证明协议

自从 2004 年采用 RSA 密码体制的 BCL DAA 方案[22]提出以后,众多的研究者对 DAA 协议进行了改进. 在相同的安全强度下,椭圆曲线密码体制比 RSA 密码体制的系统效率要高,并且具有更短的私钥和签名长度,因此椭圆曲线及其双线性对更适合于设计下一代可信计算 DAA 协议. 2008 年我们率先采用 ECC 密码体制对 DAA 协议进行了改进,提出了下一代可信计算直接匿名证明协议[27,67],大幅度提高了 DAA 协议的效率,推进了 DAA 协议的改进研究. 该方案简要概述如下:

(1) DAA-Join

① TPM/TCM 选择秘密信息 $f\in_R \mathbb{Z}/p\ \mathbb{Z}$,随机数 $t'\in_R \mathbb{Z}/p\ \mathbb{Z}$,计算 Pedersen 承诺 $C=g^f h^{t'}$,发送给 Issuer,然后 TPM/TCM 证明拥有秘密知识 f, t'.

(i) 随机选择 $r_f, r_{t'}\in_R (\mathbb{Z}/p\ \mathbb{Z})^2$,计算 $C'=g^{r_f}h^{r_{t'}}$,发送给 Issuer;

(ii) Issuer 随机选择 $c\in_R \mathbb{Z}/p\ \mathbb{Z}$,发送给 TPM/TCM;

(iii) TPM/TCM 计算 $s_f=r_f+cf, s_{t'}=r_{t'}+ct'$,发送 $s_f, s_{t'}$ 给 Issuer;

(iv) Issuer 验证 $C'\stackrel{?}{=}C^{-c}g^{s_f}h^{s_{t'}}$.

② Issuer 选择 $x\in_R \mathbb{Z}/p\ \mathbb{Z}, t''\in_R \mathbb{Z}/p\ \mathbb{Z}$,计算 $A=(g_1 C h^{t''})^{1/(\gamma+x)}$,发送 A, x, t'' 给 Host.

③ Host 存储 A, x,发送 t'' 给 TPM/TCM.

④ TPM/TCM 计算 $t=t'+t''$,存储 f, t,验证如下等式是否成立:

$$e(A, Yg_2^x)=e(g_1, g_2)e(g^f, g_2)e(h^t, g_2).$$

(2) DAA-Sign

① Host 随机选取 $w\in_R \mathbb{Z}/p\ \mathbb{Z}$,计算 $T_1=Ah^w, T_2=g^w h^{-x}$, T_1, T_2 是对 A, x 的承诺,证明如下 2 个等式成立:

$$e(T_1, Y)/e(g_1, g_2)=$$
$$e(h, Y)^w e(h, g_2)^{wx+t} e(g, g_2)^f / e(T_1, g_2)^x;$$
$$T_2=g^w h^{-x}, T_2^{-x} g^{wx} h^{-xx}=1.$$

② 证明 Host(包含 TPM/TCM)拥有知识 f, x, w, t,满足以上等式. 计算辅助值 $\delta_1=wx, \delta_2=$

$-xx$.

(i) TPM/TCM 随机选取 $r_f \in \mathbb{Z}/p\ \mathbb{Z}$, $r_t \in \mathbb{Z}/p\ \mathbb{Z}$,计算 $\tilde{R}_1$,将 $\tilde{R}_1$ 发送给 Host.

$$\tilde{R}_1 = e(g, g_2)^{r_f} e(h, g_2)^{r_t}.$$

(ii) Host 选取 $r_x, r_w, r_{\delta_1}, r_{\delta_2} \in \mathbb{Z}/p\ \mathbb{Z}$,计算:

$R_1 = \tilde{R}_1 e(h, Y)^{r_w} e(T_1, g_2)^{r_x} e(h, g_2)^{r_{\delta_1}}$;

$R_2 = g^{r_w} h^{r_x}$;

$R_3 = T_2^{r_x} g^{r_{\delta_1}} h^{r_{\delta_2}}$.

(iii) Host 计算 $c_h = H(g \| h \| g_1 \| g_2 \| g_T \| Y \| T_1 \| T_2 \| R_1 \| R_2 \| R_3)$,发送 c_h 给 TPM/TCM.

(iv) TPM/TCM 选择 $n_t \in_R \mathbb{Z}/p\ \mathbb{Z}$,计算 $c = H(H(c_h \| n_t) \| m)$.

(v) Host 计算 $s_x = r_x + c(-x)$, $s_{\delta_1} = r_{\delta_1} + c\delta_1$, $s_w = r_w + cw$, $s_{\delta_2} = r_{\delta_2} + c\delta_2$, TPM/TCM 计算 $s_f = r_f + cf$, $s_t = r_t + c(-t)$.

③ Host 输出签名是 $\sigma = (T_1, T_2, c, n_t, s_f, s_x, s_t, s_w, s_{\delta_1}, s_{\delta_2})$.

(3) DAA-Verify

① 给定消息 m 的签名 $\sigma = (T_1, T_2, c, n_t, s_f, s_t, s_x, s_w, s_{\delta_1}, s_{\delta_2})$ 和公钥 $(p, g_1, g_2, g_T, Y, g, h)$, Verifier 计算:

$$R_1' = e(g, g_2)^{s_f} e(h, Y)^{s_w} e(h, g_2)^{s_{\delta_1} + s_t} e(T_1, g_2)^{s_x} \cdot (e(T_1, Y)/e(g_1, g_2))^{-c};$$

$R_2' = T_2^{-c} g^{s_w} h^{s_x}$;

$R_3' = T_2^{s_x} g^{s_{\delta_1}} h^{s_{\delta_2}}$.

② Verifier 验证下列等式是否成立

$$c \stackrel{?}{=} H(H(H(g \| h \| g_1 \| g_2 \| g_T \| Y \| T_1 \| T_2 \| R_1' \| R_2' \| R_3') \| n_t) \| m).$$

上述方案是基于 q-SDH 假设和 DDH 假设设计的,也是最早采用双线性对和 q-SDH 假设的 DAA 方案. 文献[67]采用理想系统/现实系统模型证明该协议的安全性,主要方法是通过构造理想系统的模拟器 S 模拟协议的执行,使得环境无法区分理想系统和现实系统,从而证明该协议在 DDH 假设和 q-SDH 假设下是安全的.

该方案由于采用了椭圆曲线密码体制和双线性对,与原始 DAA 方案相比签名长度缩短 90%,计算量也显著减少,大幅度提高了 DAA 协议证明效率. 为了进一步降低 DAA Join 过程的计算量,采用上述协议类似的设计方法,我们提出了一种基于改进的 BB 签名[26]的 DAA 协议[68],将 Join 过程的计算效率提高近 1 倍.

尽管目前来看上述协议方案并不完善,知识签名的效率也不高,但是它为后来采用 q-SDH 假设构造 DAA 协议指引了方向. 后续很多研究以该方案为基础,对 DAA 协议进行了持续改进,目前这方面的研究逐渐趋于成熟.

2) 一种提供前向安全性的 DAA 协议

DAA 协议的基本安全要求就是要满足用户控制的匿名性和用户控制的可追踪性,但是对于 TPM 内部的秘密 f 泄露的安全问题考虑较少. 一旦 f 泄露不仅破坏 DAA 方案的安全性,还导致泄露之前的 DAA 签名也受到影响. 文献[69]针对这方面的问题提出了一种支持 DAA 签名前向安全性的协议,对 DAA 展开了安全性扩展研究.

前向安全性 DAA 方案在原有的 DAA 模型基础上扩展了密钥 f 更新算法,定周期地更新 f 值,以便保证即使当前 f 泄露,也无法破解之前的 DAA 签名的匿名性和不可链接性. 协议基于强 RSA 假设和 DDH 假设设计, Issuer 采用类似 CL 签名的方法为初始 f_0 颁发匿名凭证(A, e, t). TPM 的 DAA 私钥采用单向函数实施密钥周期性的更新,更新后的第 i 个周期的密钥 f_i 符合如下 DAA 匿名凭证的验证等式:

$$A^e = a^{f_i^{T-i}} b^t \bmod n.$$

DAA 签名和验证方法与原始 DAA 方法类似,不同之处在于 DAA Sign 时需要使用根离散对数知识签名方法计算关于最新周期私钥 f_i 的知识签名. 该方案在强 RSA 假设下是可证明安全的,协议不仅满足了 DAA 的基本安全属性要求,还提供了 DAA 私钥泄露后的安全增强,为 DAA 提供前向安全性保护. 目前关于 DAA 的安全性扩展和增强方面的研究还是初步的,还有许多问题值得进一步研究.

3) DAA 协议的应用拓展

DAA 方案主要是面向范围较小、边界确定的单个域的网络环境. 对于多个域的应用场景除了不能相互认证外,还可能面临跨域的中间人攻击. 我们提出了跨域的直接匿名证明方案,解决了多个信任域的 TPM 匿名认证问题[70]. 跨域 DAA 的基本思想是:如果域 A 的可信计算平台 A(Host/TPM A)要向域 B 的验证者 B(Verifier B)证明平台身份. 那么首先平台 A 向本地的护照颁发者申请一个护照证书,该护照证书证明了可信平台 A 在信任域 A 中的身份. 然后可信计算平台 A 用申请到的护照证书向信任域 B 的签证颁发者申请签证证书. 最后,可信计算平台 A 用护照证书和签证证书向信任域 B 中的验证者 B 匿名地证明平台 A 的身份. 系统结构如

图3所示.跨域DAA协议的主要改进工作是在原有的DAA协议上扩展了IDAA-IssuePassport和IDAA-IssueVisa这2个用于获取护照证书和获取签证证书协议流程.

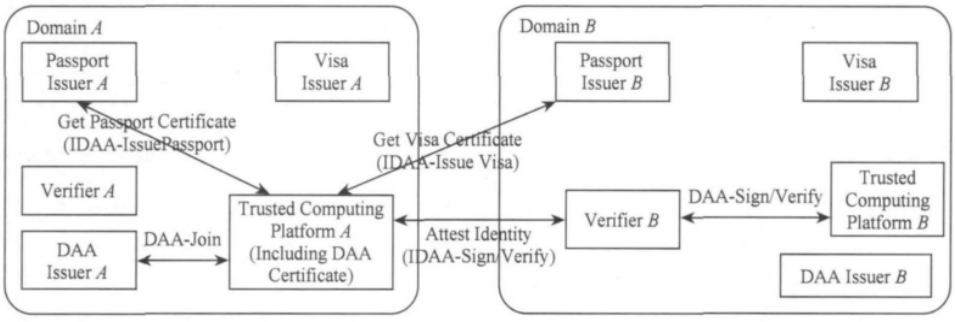

Fig. 3 Inter-domain DAA architecture.

图3 跨域DAA架构

除此之外,DAA协议还能应用于无线终端、手机和其他嵌入式设备,DAA协议要适应这些应用场景还有很大的改进空间,有待于进一步深入研究.

2.2.2 基于属性的远程证明

平台完整性证明是可信计算领域最重要的研究问题之一,目前已有众多的解决方案.在这些方案中,基于属性的远程证明发展前景最广阔,实用价值最高.我们从证明粒度、证明效率以及与DAA相结合3个方面对基于属性的远程证明开展了系统研究[71-73].

1) 细粒度的组件属性远程证明方案

原始的PBA协议[36]证明的是整个平台总体属性,这种粗粒度的属性在实际应用中面临属性评估困难、撤销频繁的问题.针对这些不足,我们通过测试评估系统软硬件组件属性,改进并实现了基于组件属性的远程证明协议及其系统[73].组件属性证明的基本思想是将系统属性证明请求转化为若干组件的属性逻辑表达式,依次证明每个组件满足特定的组件属性.组件属性证明采用零知识证明的方法,证明平台组件度量结果的承诺满足组件预置的属性证书要求,整个方案在随机预言模型下可证明是安全的.组件属性证明系统中,首先TPM对组件度量进行承诺并签名,然后主机随机化CL组件属性证书,向验证方证明TPM承诺的组件完整性配置符合证明的组件属性要求,最后验证方在属性权威机构的协助下验证属性是否撤销、承诺签名是否有效等.

基于组件属性的远程证明方案其特点是:①属性粒度细、验证方便、扩展性强;②无需临时颁发属性证书,属性撤销和验证简单高效;③保护平台组件的隐私.组件属性证明方案将基于属性的远程证明的研究向前推进了一步,从协议构造和系统实现2方面解决了属性远程证明应用的基本问题.

2)基于双线性对的高效属性证明协议

传统的采用RSA密码体制构建基于属性的远程证明协议存在零知识证明计算量大、效率低的不足,文献[71]采用双线性对在TCM密码算法的支持下构建了一种高效的属性证明协议.双线性对的属性证明协议的安全模型与传统RSA属性证明模型完全相同,要求满足证明不可伪造和配置隐私保护的安全属性.该协议通过为平台配置属性对(cs, ps)颁发CL-LRSW双线性对的属性证书$\sigma=(a, A, b, B, c)$来标识平台属性,平台采用知识签名证明平台的配置承诺、随机化的属性证书与TCM证明绑定,也即是如下证明公式:

$$SPK\{(cs, r_0, r, t_1, t_2) \mid v_x v_{xy}^{cs} v_{xyz}^{ps} = v_s^r \wedge C = g_T^{cs} h_T^{r_0} \wedge d_1 = X^{t_1} \wedge d_2 = Y^{t_2}\}(N_v, N_t).$$

该协议方案采用双线性对简化了属性远程证明,并从远程证明的不可伪造性和配置隐私保护2方面证明了协议的安全性.方案与原有PBA协议相比,证明计算量减少约32%,签名长度减短约63%.

3) PBA与DAA相结合的匿名属性证明协议

直接匿名证明和基于属性的证明是远程证明的2方面的功能,实际应用中必须是两者高效的相互结合,就是在同一个证明流程中同时完成直接匿名证明和属性证明.文献[72]在PBA和DAA结合研究方面提出了一种高效的证明方案.该方案的基本思想是将DAA的匿名身份认证暗含于基于属性的远程证明过程中,可信第三方首先验证DAA匿名身份,然后再颁发关于匿名身份和平台配置属性对(f, cs, ps)的属性证书,这样的优势在于证明过程只需一次属性远程证明协议就能完成远程证明,而无需再运行直接匿名证明协议了.

匿名属性证明协议采用序列游戏(sequence of game)的方法证明了协议的安全性,该协议同时满足不可伪造性、平台身份的匿名性以及平台配置的隐私保护等安全属性.匿名属性证明协议的计算量提升显著,性能对比分析结果参照表1(S表示平方(square)计算,M表示模幂(multiexponent)计算,P表示对(paring)计算).

Table 1 Computation Analysis on the Anonymous Property-Based Attestation Protocol

表1 匿名属性证明协议计算量分析表

Analysis Item	DAA + PBA Scheme	Our APA Scheme
Attest Phase	30 673 S+16 351 M	3 390 S+1 699 M
Verify Phase	23 651 S+11 844 M	2 480 S+1 247 M+15 P
Signature Length/B	2 972	849

基于属性的远程证明研究已经取得了许多重要的研究进展,解决了PBA的基本关键问题,但这方面研究的深度和广度都还不够,需要开展更深入的研究.

2.3 可信网络连接

现有可信网络连接方面的研究都是基于TCG的TNC架构展开的.TNC架构通过对接入终端的完整性和平台身份鉴别,保证接入网络终端平台身份和状态的可信,继而保证整个网络环境的可信.但是,目前的TNC解决方案还存在终端平台身份的隐私保护问题、TNC架构中各实体之间交互的安全协议支持问题、网络接入后的安全保护问题等.我们针对终端平台接入网络时的身份隐私问题,基于TNC架构提出了一种平台匿名网络接入控制方法[74],研发了一套LOIS可信网络接入系统.

LOIS可信网络接入系统架构如图4所示,其由终端域、策略实施域、策略决策域和服务域构成.策略实施域根据策略决策域的判定结果实施网络接入控制.策略决策域主要由网络接入控制服务器、平台身份管理服务器和平台完整性管理服务器等构成.网络接入控制服务器根据网络接入控制策略实施基于终端平台身份和完整性的细粒度接入控制,支持针对终端设备及用户的差异化网络接入管理.网络接入控制服务器还能够提供终端接入审计信息查询,为接入终端动态监控和追踪提供服务支撑.最新的TNC规范采用MAP加强了对接入终端管控,本系统中采用终端平台身份和完整性信息作为终端元数据标识,通过这些标识通知网络接入控制服务器对异常行为的终端实施主动网络控制.平台完整性管理服务器负责管理终端平台固件、系统软件和应用软件等的完整性度量基准值.平台身份管理服务器负责管理终端平台身份凭证的颁发、验证和撤销,在本系统中同时支持普通平台身份证书和平台匿名身份凭证2种方式.

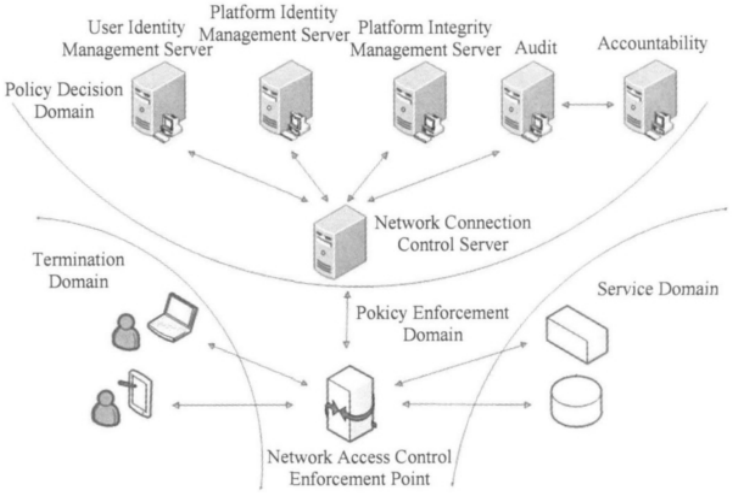

Fig. 4 Lois trusted network connection system architecture.

图4 LOIS可信网络接入系统架构

针对平台终端隐私保护的问题,我们在TCG的TNC架构基础上,借鉴直接匿名证明的思想,提出了一种平台匿名网络接入控制方法.接入前终端平台需向平台身份管理服务器申请匿名凭证DAACert.我们扩展了终端可信网络接入时流程的第4步和第6步的功能[45](平台凭证验证阶段),实现终端平台的匿名网络接入.在平台匿名接入的第4步,终端平台根据DAACert计算平台匿名身份密钥的知识签名,将

签名结果发送至平台身份管理服务器验证以便获得匿名身份密钥的认证凭证.在平台匿名接入的第6步,终端平台使用经过平台身份管理服务器认证的匿名身份密钥对平台完整性度量值进行签名,然后网络接入控制服务器验证终端平台匿名身份的真实性和平台完整性度量值的正确性.

TNC将终端平台信任延伸至网络空间,但没有考虑到网络接入时的终端平台身份隐私.LOIS可信网络接入系统将TNC和DAA相结合,有效监控网络接入终端的同时注重保护其隐私,满足了开放式网络接入的安全需求.

2.4 可信计算应用

可信计算可广泛应用于安全主机、可信网络、数据存储和数字版权管理等方面.我们重点关注了可信存储和可信使用控制,利用可信计算技术保证数据存储的机密性和新鲜性,并实现数据的可信使用控制.

2.4.1 可信存储

在TCG可信计算框架下,TPM的封装功能将存储数据与PCR中的系统配置绑定,保证存储数据的机密性安全.由于系统硬件、软件频繁更新会导致封装数据的不可用,TCG封装存储方案的应用受到很大局限.为此,我们研究提出了一个应用于虚拟平台的属性封装方案[75],该方案利用一个TPM同时保护多个虚拟机系统的数据安全,通过对属性的分级处理增强了封装数据使用的灵活性.在该方案中,每个虚拟机都对应一组虚拟PCR(vPCR)存储其系统配置.封装时,将虚拟机的系统配置映射转化为安全属性,并将属性值动态扩展至可重置PCR中,由TPM实施数据与系统属性的封装;解封装时,先比较当前系统属性与封装时系统属性的安全级别,并扩展相应的属性值到可重置PCR中,然后由TPM实施解封装操作.通过这种方式保证封装存储数据只有在其系统属性安全级别不降低的情况下才能解封使用.

TCG将存储数据与TPM中的单调计数器绑定,从硬件层保证数据的新鲜性,防止重放攻击.但是TPM由于价格与工艺等问题只能提供少量硬件计数器,根本无法满足应用中大量存储数据的新鲜性要求.因此,我们研究提出了一种虚拟单调计数器构建方案[76],在TPM硬件计数器的基础上构建与之绑定的虚拟计数器,利用TPM硬件特性保证虚拟计数器的算术增长性、防篡改性等.在该方案中,虚拟计数器的创建及增加操作都会触发TPM计数器的增加操作,其中TPM计数器的增加操作是由TPM的传输会话来保障其安全,而其传输会话日志记录了TPM计数器和虚拟计数器的操作,由此实现虚拟计数器与TPM计数器的绑定.虚拟计数器日志记录不仅包含虚拟计数器和TPM计数器的操作,还包含TPM传输会话日志,通过检查该日志记录中的相关信息可以保证虚拟计数器读取操作时虚拟计数器的可信性.虚拟计数器方案的安全性仅依赖于硬件TPM,其算术单调性可以有效地应用于多种可信存储场景.

针对可信存储中的众多安全问题,我们从数据机密性和新鲜性的角度,利用可信计算技术给出了属性封装和虚拟单调计数器的解决方案.而结合可信计算技术从硬件层解决可信存储中的其他安全问题,有待进一步挖掘研究.

2.4.2 可信使用控制

在分布式应用中,数据的使用不再局限于本机,必须保证在任何分布式终端上数据都能按照数据所有者的要求被安全使用.我们利用可信计算技术研发了一个可信使用控制系统[77-78],综合考虑了策略的表述能力,数据和策略在分发、使用时的安全性,保证数据使用者严格按照数据所有者制定的策略来使用数据.

数据所有者将数据和使用控制策略分发给数据使用者时,需要验证其系统环境是否满足要求,因此分发过程不仅要保证数据和策略的安全,还要保证数据使用者系统配置的隐私性.在可信使用控制系统中,我们基于TLS安全信道传输数据和策略保证其机密性和认证性,采用密钥认证的方式验证数据使用者系统配置以保护其隐私[77].数据所有者拥有一个可信配置集,凡属于该集合的系统配置均被认为其满足安全策略要求,可以向其对应系统分发数据.数据使用者在请求数据时,先利用TPM/TCM产生一个加密密钥,计算其承诺并对该承诺签名,然后根据该承诺以及与该密钥绑定的可信配置集派生出一个环签名的私钥,利用环签名和TPM/TCM对承诺的签名证明该私钥使用环境的可信性.数据所有者接收到请求后,验证环签名和TPM/TCM对承诺的签名,再利用上述加密密钥加密数据和策略发送给数据使用者.由于TPM/TCM的承诺以及环签名的难以伪造性,所以不需要泄露数据使用者的系统配置,数据所有者可直接验证其可信性从而控制数据的可信分发.

数据使用者接收到分发的数据和策略之后,必须先对其安全存储,然后根据策略控制对数据的使用.

可信使用控制系统以数字信封的方式加密存储数据,数字信封的密钥由 TPM/TCM 封装保护,并且该密钥与策略作为标签以扩展属性的方式与数据绑定[78].对数据实施使用控制时,首先利用 LSM 钩子函数截获进程对数据的读、写操作请求,然后利用动态度量模块获取进程的完整性状态,并根据策略判定数据的访问请求,如果允许则解密获取数据.

针对现实生活中的具体场景,我们利用可信使用控制系统提出了基于 TPM 的数字版权管理方案[79]和数字内容分层使用控制方案[80].

2.5 可信计算测评

目前可信计算测评已经成为可信计算领域的研究热点,其研究主要集中于 2 个方面:一是 TPM/TCM 规范符合性自动化测试.相对于传统的手工方法,自动化测试不但成本低、效率高,而且支持良好的结果分析(如测试覆盖度统计),便于量化测试结果的可信度.二是可信计算协议分析评估.传统分析工作主要关注密码协议,近年来系统分析工作逐渐兴起,成为新的发展方向.

2.5.1 TPM/TCM 规范符合性自动化测试

德国波鸿鲁尔大学给出了第 1 个 TPM 规范符合性测试方案,该方案的实施需要大量的手动操作和特定的专业知识,而且缺乏有效的测试结果分析.鉴于这种情况,我们建立了基于扩展有限状态机(extended finite state machine, EFSM)的 TPM/TCM 测评模型,提出了 TPM/TCM 规范符合性自动化测评方法[81-82],并在该方法的基础上研发了可信计算平台测评系统.

1) TPM/TCM 测评模型

建立 TPM/TCM 形式化测评模型是可信计算测评的基础.我们利用 Z 语言对 TPM/TCM 安全芯片抽象进行形式化描述,从而建立其扩展有限状态机模型.

TPM/TCM 的规范都以自然语言表述,容易造成歧义.针对这方面的问题,我们使用 Z 语言形式化描述了 TPM/TCM 规范,例如,图 5 展示了使用 Z 语言描述的密钥生成、导入、导出操作流程.这种描述方式准确的定义了 TPM/TCM 的功能和操作.

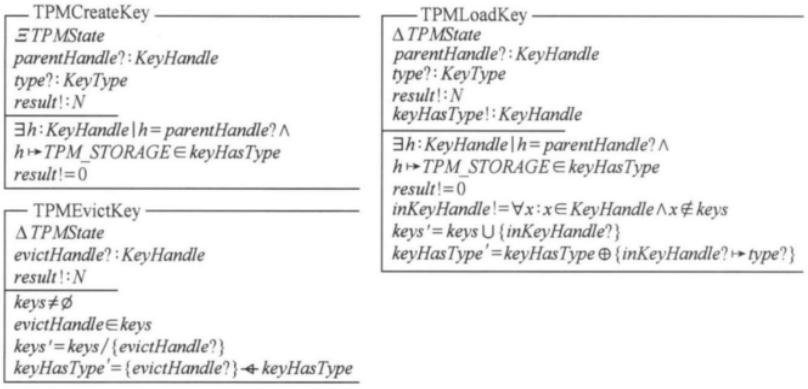

Fig. 5 Formal description for key operation.

图 5 密钥操作的形式化描述

在 Z 语言描述的基础上,我们给出了基于 EFSM 的 TPM/TCM 测评模型. EFSM 定义为一个六元组$\langle S, S_0, I, O, T, V\rangle$,其中 S 是一个非空的状态集合,S_0 是初始状态,I 是一个非空的输入消息集合,O 是一个非空的输出消息集合,V 是变量集合,对于任意的 $t\in T$,t 是一个六元组(s, x, P, op, y, s'),其中 $s, s'\in S$ 分别是初始状态和终止状态;$x\in I$ 是状态迁移 t 的输入;$y\in O$ 是状态迁移 t 的输出;P 是状态迁移 t 的前置条件,可能为空;op 是状态迁移中的操作,其中由一系列的输出语句和变量赋值语句组成.我们采用上述自动机定义建立了 TPM/TCM 的测评模型,以 TPM/TCM 密码学子系统为例,其模型如图 6.

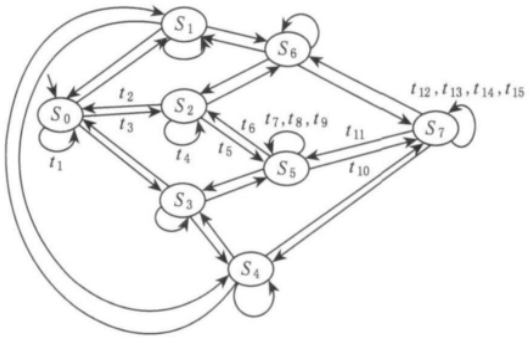

Fig. 6 EFSM model for TPM/TCM cryptography system.

图 6 TPM/TCM 密码学子系统的 EFSM 模型

该模型通过 EFSM 状态变量描述了与 TPM/

TCM 状态相关的内部变量,并采用增加约束条件的方法大幅度减少状态变量组合数,既避免了状态空间爆炸,同时又有效地描述了 TPM 状态转化.

2) TPM/TCM 自动化测评方法

在上述模型的基础上,我们首先对 TPM/TCM 进行了命令依赖关系分析,然后再提出基于规约的测试用例自动生成方法,形成了 TPM/TCM 自动化测评方法,如图 7 所示:

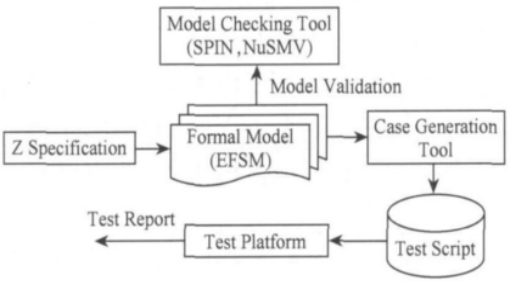

Fig. 7 TPM/TCM test flow.

图 7 TPM/TCM 测评流程

TPM/TCM 命令依赖关系分析分为 2 方面:一是给出命令之间的数据流和控制流关系;二是划分各个功能模块并给出功能模块之间的依赖关系. 我们定义命令 $Command_A$ 依赖于命令 $Command_B$,当且仅当:①命令之间存在数据流依赖关系,也就是 $Command_B$ 为 $Command_A$ 提供数据,例如 TPM_LoadKey 命令为 TPM_Seal 提供密钥参数;或②命令之间存在控制流依赖关系,也就是 $Command_B$ 为 $Command_A$ 提供执行保障,例如必须先执行 TPM_TakeOwnership 才能执行 TPM_CreateWrapKey. 我们再定义 TPM/TCM 功能模块 $Module_A$ 依赖于 $Module_B$,当且仅当 $Module_A$ 中存在命令 $Command_A$,$Command_A$ 依赖于 $Command_B$ 且 $Command_B$ 属于 $Module_B$.

在详细的命令依赖关系分析的基础上,我们提出基于规约的测试用例自动生成方法. 用例生成主要分为 2 个阶段:第 1 阶段根据命令依赖关系确定测试用例中的 TPM/TCM 命令执行流程,生成抽象测试用例,同时采取裁剪操作结果非法项和等价项的方式对抽象测试用例进行规约,抽象测试用例不能直接执行;第 2 阶段生成具体测试用例,主要根据实际需求中的限制条件来具体化测试输入,最后采用测试用例生成工具自动化生成具体的测试用例. 用例生成之后,通过使用 TPM/TCM 安全芯片用例可达性分析树对测试用例路径进行有效性分析,进一步验证测试用例的覆盖度.

3) 可信计算平台测评系统

基于上述 TPM/TCM 自动化测评方法,我们研制了可信计算平台测评系统. 该系统以我国自主的可信计算标准[5]为指导,支持可信计算平台密码算法和协议的标准符合性、正确性和性能检测,以及可信计算平台的安全功能和接口标准符合性、安全性和实现特性的检测,提供测试报告自动生成、测试覆盖度有效性分析等功能,易于测试用例的扩展. 可信计算平台测评系统是国内第 1 套投入实际应用的可信计算产品检测平台. 表 2 是用该检测平台测试的国内某 TCM 产品的抽样测试结果.

Table 2 Test Result of Some TCM Sample

表 2 国内某款 TCM 抽样测试结果

Functional Modules	Test Cases	Errors	Pass Rate/%
Context	24	4	83.3
Policy	23	1	95.7
TCM	38	12	68.4
Key	23	9	60.9
Data	14	2	85.7
PCR	10	4	60.0
NV	10	3	70.0
Hash	12	4	67.7
TOTAL	154	39	74.7

依据上述严谨的理论研究,通过大量检测实践工作验证,我们还形成了 2 项可信计算测评标准:《可信密码模块符合性测试标准》和《可信密码模块保护轮廓标准》,这 2 项标准对指导国内可信计算产品生产、测评、认证都发挥了关键作用.

2.5.2 可信计算协议分析评估

可信计算协议分析评估方面,我们重点研究 TCM 授权协议的安全性分析,利用模型检测技术对 TCM 的核心机制——授权会话协议(authorization protocol, AP)——进行了全面分析[60].

我们首先建立 AP 协议及其环境威胁的模型的 PROMELA(process meta language). 该模型中存在 3 个角色:用户 U,攻击者 A 和 TCM. 同时引入 2 个半双工管道:U_to_A 和 A_to_TCM. 攻击者 A 位于 U 和 TCM 之间,分别通过管道与 U 及 TCM 通信,A 可以拦截、篡改和自主发送管道中的任何消息. 根据上述模型,可以利用 SPIN 工具对 AP 协议进行检测. 检测前首先需要指定协议的运行方式,我们规定了 2 个会话(表征攻击者与 TCM 和 U 之间的通信)和 3 个协议参与方行为模式.

根据 SPIN 工具测试结果,我们发现了 2 种可能的攻击:重放攻击和离线字典攻击.

在重放攻击中,攻击者先按照 AP 协议流程产生 AP 会话,但在执行命令时截获命令参数并保存,然后强行中断与用户的会话. 当用户重新建立会话后,攻击者可以重放保存的原有会话信息并成功执行命令. 为避免上述攻击,可以在 TCM 内增加 1 个计数器用于维持 AP 会话计数,如图 8 所示. 每执行 1 次会话,计数器值加 1,会话执行前必须验证计数器值是否匹配,重放攻击会因计数器值失效而失败.

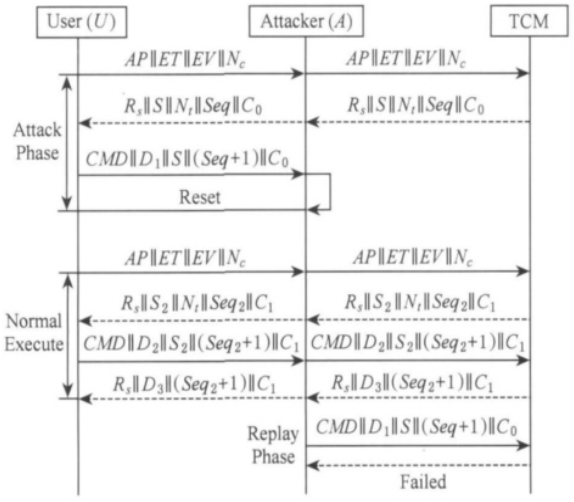

Fig. 8 Method of preventing replay attack.

图 8 针对重放攻击的防范方法

在离线字典攻击(如图 9 所示)中,假设 A 已经获得了共享秘密数据(AP 协议中的 ShareSecret). 如果每次会话开始时使用的序列号 Seq 不是随机的,则 A 可能离线猜测 Seq,一旦得到 Seq 值则可以执行任何 TCM 命令.

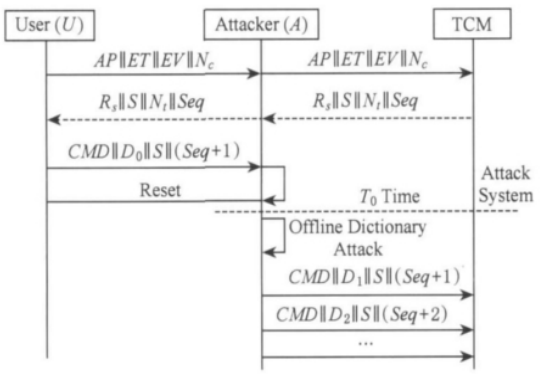

Fig. 9 Offline dictionary attack on AP protocol.

图 9 针对 AP 协议的离线字典攻击

经过我们对国内 TCM 芯片授权协议实现的测试,发现 TCM 芯片对密钥句柄的产生是有序的,新产生的密钥句柄缺少了新鲜性的保证. 如果攻击者有能力从 TCM 中释放一个密钥,攻击者就能够猜测到新加载密钥的句柄,从而造成中间人攻击.

不过,上述这些安全隐患都是理论上的,通过采用简单的安全措施比较容易克服.

3 结束语

可信计算作为一种新型的安全支撑技术,已经成为信息安全领域的研究热点. 产业化方面国际上主流的台式机、笔记本都已经标配上了 TPM 安全芯片,国内支持 TCM 安全芯片的安全主机已经全面量产. 尽管可信计算产业发展取得重大进展,但是在研究领域可信计算理论和关键技术还面临很多问题需要解决[83]. 2007 年国内专家曾指出可信计算发展中面临 5 方面的难题[84],随着近几年国内外可信计算研究的深入[85],在某些方面的问题上,可信计算理论和关键技术已经取得了一定的突破.

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,提出了基于信息流的动态度量方法,采用动态度量技术与进程信息流访问控制相结合的方法构建了平台信任.

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. 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.

可信计算无疑是一项拥有广阔应用前景的安全技术,但在现实中它并不是一种解决所有 IT 安全问题的"万能药". 当前发展过程中可信计算还面临一些挑战,这阻碍了它的全面应用. 主要挑战有:1)可信计算理论模型研究发展相对缓慢,近年来未能实现大的突破;2)可信计算安全芯片的功能过于复杂,其兼容性和标准符合性还未得到很好解决;3)可信计算核心关键技术实施存在管理复杂、扩展性不好的

问题;4)与操作系统、网络和应用安全机制的融合不够深入.

但是我们坚信随着国内外研究的深入,以及信息安全技术的自身发展,阻碍可信计算发展的瓶颈问题一定能够逐步得到解决,从长远看可信计算必定是未来信息安全技术发展的重要突破方向.我国目前已经处在国际可信计算研究领域的前列,我们应该抓住机遇,持续推进可信计算技术和产业的发展,有效提升我国信息安全总体水平,保障国家重要信息系统的安全.

参 考 文 献

[1] China Internet Network Information Center. 2005 Survay report of Chinese internet security [EB/OL]. 2005. [2011-01-25]. http://www.cnnic.net.cn

[2] Common Criteria Project Sponsoring Organisation. Common criteria for information technology security evaluation. ISO/IEC International Standard 15408 version 2.1 [S]. Genevese: Common Criteria Project Sponsoring Organisation, 1999

[3] Avizienis A, Laprie J C, Randell B, et al. Basic concepts of dependable and secure computing [J]. IEEE Trans on Dependable and Secure Computing, 2004, 1(1): 11-33

[4] Trusted Computing Group. TCG specification architecture overview, version 1.2 [EB/OL]. 2003. [2011-01-25]. https://www.trustedcomputinggroup.org

[5] China State Password Administration Committee. Technic specification of cryptographic supporting platform for trusted computing [EB/OL]. 2007. [2011-01-25]. http://www.oscca.gov.cn/ (in Chinese)
(国家密码管理局. 可信密码支撑平台技术规范[EB/OL]. 2007. [2011-01-25]. http://www.oscca.gov.cn/)

[6] Trusted Computing Group. TPM main specification, version 1.2 [EB/OL]. 2003. [2011-01-25]. https://www.trustedcomputinggroup.org

[7] Microsoft. Security model for the next-generation secure computing base [EB/OL]. 2002. [2011-01-25]. http://www.microsoft.com/resources/ngscb/documents/ngscb_security_model.doc

[8] Intel. Trusted execution technology architecture overview [EB/OL]. 2003. [2011-01-25]. http://www.intel.com/technology/security/arch-overview.pdf

[9] Petroni NJr, Fraser T, et al. Copilot—A coprocessor-based kernel runtime integrity monitor [C] //Proc of the 13th Conf on USENIX Security Symposium. Berkeley: USENIX, 2004: 179-194

[10] Seshadri A, Luk M, Shi E, et al. Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems [C] //Proc of the 12th ACM Symp on Operating Systems Principles. New York: ACM, 2005: 1-16

[11] Sailer R, Zhang Xiaolan, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture [C] //Proc of USENIX Security'04. Berkeley: USENIX, 2004: 223-238

[12] Jaeger T, Sailer R, Shankar U. PRIMA: Policy-reduced integrity measurement architecture [C] //Proc of the 11th ACM Symp on Access Control Models and Technologies. New York: ACM, 2006: 19-28

[13] Shi E, Perrig A, Doorn L V. BIND: A fine-grained attestation service for secure distributed systems [C] //Proc of the 2005 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Computer Society, 2005: 154-168

[14] Peng Guojun, Pan Xuanchen, Zhang Huanguo, et al. Dynamic trustiness authentication framework based on software's behavior integrity [C] //Proc of the 9th Int Conf for Young Computer Scientists (ICYCS 2008). Los Alamitos, CA: IEEE Computer Society, 2008: 2283-2288

[15] Xu Ziyao, He Yeping, Deng Lingli. An integrity assurance mechanism for run-time programs [C] //Proc of Information Security and Cryptology. Berlin: Springer, 2009: 389-405

[16] Loscocco PA, Wilson PW, Pendergrass JA, et al. Linux kernel integrity measurement using contextual inspection [C] //Proc of the 2nd ACM Workshop on Scalable Trusted Computing. New York: ACM, 2007: 21-29

[17] Azab AM, Ning P, Sezer EC, Zhang X. HIMA: A hypervisor-based integrity measurement agent [C] //Proc of the 2009 Annual Computer Security Applications Conf. Los Alamitos, CA: IEEE Computer Society, 2009: 461-470

[18] Azab AM, Ning Peng, Wang Zhi, et al. HyperSentry: Enabling stealthy in-context measurement of hypervisor integrity [C] //Proc of the 17th ACM Conf on Computer and Communications Security. New York: ACM, 2010: 38-49

[19] Berger S, Cáceres R, Goldman K A, et al. vTPM: Virtualizing the trusted platform module [C] //Proc of the 15th USENIX Security Symposium. Berkeley: USENIX, 2006: 305-320

[20] Sadeghi AR, Stüble C, Winandy M. Property-based TPM virtualization [C] //Proc of the 11th Int Conf on Information Security. Berlin: Springer, 2008: 1-16

[21] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols [C] //Proc of 3rd Int Conf Security in Communication Networks. Berlin: Springer, 2003: 268-289

[22] Brickel E, Camenisch J, Chen L. Direct anonymous attestation [C] //Proc of the ACM Conf on Computer and Communications Security. New York: ACM, 2004: 132-145

[23] He Ge, Tate SR. A direct anonymous attestation scheme for embedded devices [C] //Proc of Public Key Cryptography. Berlin: Springer, 2007: 16-30

[24] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentialsfrom bilinear maps [C] //Proc of CRYPTO 2004. Berlin: Springer, 2004: 56-72

[25] Brickel E, Chen Liqun, Li Jiangtao. A new direct anonymous attestation scheme from bilinear maps [C] //Proc of Trusted Computing-Challenges and Applications. Berlin: Springer, 2008: 166-178

[26] Boneh D, Boyen X. Short signatures without random oracles [C] //Proc of EUROCRYPT 2004. Berlin: Springer, 2004: 56-73

[27] Chen Xiaofeng, Feng Dengguo. Direct anonymous attestation for next generation TPM [J]. Journal of Computers, 2008, 43(50): 43-50

[28] Chen Liqun, Morrissey P, Smart N P. DAA: Fixing the pairing based protocols, PB 2009/198 [R/OL]. 2009. [2009-05-20]: http://eprint.iacr.org/2009/198

[29] Chen Liqun. A DAA scheme using batch proof and verification [C] //Proc of the 3rd Int Conf on Trust and Trustworthy Computing. Berlin: Springer, 2010: 166-180

[30] Chen Liqun, Page D, Smart N P. On the design and implementation of an efficient DAA scheme [C] //Proc of Smart Card Research and Advanced Application Conf CARDIS 2010. Berlin: Springer, 2010: 223-238

[31] Sailer R, Doorn V L, Ward J P. The role of TPM in enterprise security, PB RC23363 [R]. New York: IBM, 2004

[32] Poritz J, Schunter M, Herreweghen E V, et al. Property attestation scalable and privacy friendly security assessment of peer computer, PB RZ3548 [R]. New York: IBM, 2004

[33] Sadeghi A R, Stüble C. Property-based attestation for computing platforms: Caring about properties, not Mechanisms [C] //Proc of the 2004 Workshop on New Security Paradigms. New York: ACM, 2004: 67-77

[34] Chen Liqun, Landfermann R, Löhr H, et al. A protocol for property-based attestation [C] //Proc of the 2006 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2006: 7-16

[35] Kühn U, Selhorst M, Stüble C. Realizing property-based attestation and sealing with commonly available hard- and software [C] //Proc of the 2007 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2007: 50-57

[36] Chen Liqun, Lohr H, Manulis M, et al. Property-based Attestation without a Trusted Third Party [C] //Proc of the 11th Int Conf on Information Security. Berlin: Springer, 2008: 31-46

[37] Haldar V, Chandra D, Franz M. Semantic remote attestation: A virtual machine directed approach to trusted computing [C] //Proc of USENIX Virtual Machine Research and Technology Symp. Berkeley: USENIX, 2004: 29-41

[38] Seshadri A, Perrig A, Doorn L V, et al. SWATT: Software-based attestation for embedded devices [C] //Proc of the IEEE Security & Privacy Conf. Los Alamitos, CA: IEEE Computer Society, 2004: 272-282

[39] Li Xiaoyong, Zuo Xiaodong, Shen Changxiang. System behavior based trusteworthiness attestation for computing platform [J]. Acta Electronica Sinica, 2007, 35(7): 1234-1239 (in Chinese)
(李晓勇, 左晓栋, 沈昌祥. 基于系统行为的计算平台可信证明[J]. 电子学报, 2007, 35(7): 1234-1239)

[40] Neumann P G. Principled assuredly trustworthy composable architectures [EB/OL]. 2004. [2011-01-25]. http://www.csl.sri.com/neumann/chats4.html.

[41] Ellison R J, Moore A P. Trustworthy refinement through intrusion-aware design (TRIAD), PB ADA414865 [R]. Pittsburgh: Software Engineering Institute, 2002

[42] Lin Chuang, Peng Xuemei. Research on trusted network [J]. Chinese Journal of Computer, 2005, 28: 751-758 (in Chinese)
(林闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28(5):751-758)

[43] Cisco System. Network admission control (NAC) executive overview [EB/OL]. 2009. [2011-01-25]. http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns617/net_implementation_white_paper0900aecd8051fc24.pdf

[44] Microsoft Corporation. Network access protection platform architecture [EB/OL]. 2008. [2011-01-25]. http://download.microsoft.com/download/3/9/f/39ff0ca3-56d1-4d93-af46-98f92134d040/NAPArch.doc

[45] Trusted Computing Group. TNC architecture for interoperability [EB/OL]. [2011-01-25]. http://www.trustedcomputinggroup.org/resources/tnc_architecture_for_interoperability_specification

[46] Zhang Huanguo, Chen Lu, Zhang Liqiang. Research on trusted network connection [J]. Chinese Journal of Computer, 2010, 33(4): 706-717 (in Chinese)
(张焕国, 陈璐, 张立强. 可信网络连接研究[J]. 计算机学报, 2010, 33(4): 706-717)

[47] Goldman K, Perez R, Sailer R. Linking remote attestation to secure tunnel endpoints [C] //Proc of the 2006 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2006: 21-24

[48] Gasmi Y, Sadeghi A R, Stewin P, et al. Beyond secure channels [C] //Proc of the 2007 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2007: 30-40

[49] Armknecht F, Gasmi Y, Sadeghi A R, et al. An efficient implementation of trusted channels based on openssl [C] //Proc of the 2008 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2008: 41-50

[50] Sadeghi A R, Selhorst C, Stüble C, et al. TCG inside?—A note on TPM specification compliance [C] //Proc of the 2006 ACM Workshop on Scalable Trusted Computing. New York: ACM, 2006: 47-56

[51] Cui Qi, Shi Wenchang. An approach for compliance validation of TPM through applications [J]. Journal of the Graduate School of the Chinese Academy of Sciences. 2008, 25(5): 649-656 (in Chinese)
(崔奇, 石文昌. 一种通过应用程序验证TPM标准符合性的方法[J]. 中国科学院研究生院学报, 2008, 25(5): 649-656)

[52] Zhang Huanguo, Yan Fei, Fu Jianming, et al. Research on theory and key technology of trusted computing platform security testing and evaluation [J]. Science in China: Series F Information Sciences, 2010, 53(3): 434-453 (in Chinese)
(张焕国, 严飞, 傅建明, 等. 可信计算平台测评理论与关键技术研究[J]. 中国科学: F辑信息科学, 2010, 40(2): 167-188)

[53] Trusted Computing Group. TCG certification program announcement [EB/OL]. [2011-01-25]. http://www.infineon.com/cms/en/corporate/press/news/releases/2009/INFCCS200912-015.html; http://www.trustedcomputinggroup.org/certification

[54] Trusted Computing Group. Protection profile of PC client specific trusted platform module TPM Family 1.2 [EB/OL]. [2011-01-25]. http://www.trustedcomputinggroup.org/resources/tpm_12_protection_profile/

[55] Trusted Computing Group. Security conformance evaluation of the infineon TPM confirmed by common criteria certificate [EB/OL]. [2011-01-25]. http://www.infineon.com/cms/en/corporate/press/news/releases/2009/INFCCS200912-015.html

[56] Bruschi D, Cavallaro L, Lanzi A, et a1. Replay attack in TCG specification and solution [C] //Proc of the 21st Annual Computer Security Applications Conf. Los Alamitos, CA: IEEE Computer Society, 2005: 438-453

[57] Chen Liqun, Ryan M. Attack. Solution and verification for shared authorisation data in TCG TPM [C] //Proc of the 6th Workshop on Formal Aspects in Security and Trust. Berkeley: USENIX, 2005: 201-216

[58] Backes M, Maffei M, Unruh D. Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol [C] //Proc of the 2008 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Computer Society, 2008: 202-215

[59] Datta A, Franklin J, Garg D, et al. A logic of secure systems and its application to trusted computing [C] //Proc of the 2009 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Computer Society, 2009: 221-236

[60] Chen Xiaofeng, Feng Dengguo. Model checking of trusted cryptographic module [J]. Journal on Communications, 2010, 31(1): 59-65 (in Chinese)
(陈小峰, 冯登国. 可信密码模块的模型检测分析[J]. 通信学报, 2010, 31(1): 59-65)

[61] Chen Jun. Security analysis and application of trusted platform module [D]. Beijing: Institute of Computing Technology, Chinese Academy of Science, 2006 (in Chinese)
(陈军. 可信平台模块安全性分析与应用[D]. 北京: 中国科学院计算技术研究所, 2006)

[62] Wang Dan, Feng Dengguo. Trustworthiness-based trust chain model [C] //Proc of the 7th China Conf on Information and Communications Security. Beijing: Science Press, 2010: 1-5 (in Chinese)
(汪丹, 冯登国. 基于信任度的信任链模型[C] //第七届中国信息与通信安全学术会议. 北京: 科学出版社, 2010: 1-5)

[63] Nie Xiaowei, Feng Denguo. Modified security model based on dynamic trusted degree [J]. Journal on Communications, 2008, 29(10): 37-44 (in Chinese)
(聂晓伟, 冯登国. 基于动态可信度的可调节安全模型[J]. 通信学报, 2008, 29(10): 37-44)

[64] Liu Ziwen, Feng Dengguo. TPM-based dynamic integrity measurement architecture [J]. Journal of Electronics & Information Technology, 2010, 32(4): 875-879 (in Chinese)
(刘孜文, 冯登国. 基于可信计算的动态完整性度量架构[J]. 电子与信息学报, 2010, 32(4): 875-879)

[65] Hu Hao, Feng Dengguo. BIFI: Architectural support for information flow integrity measurement [C] //Proc of 2008 Int Conf on Computer Science and Software Engineering. Los Alamitos, CA: IEEE Computer Society, 2008: 605-609

[66] Qin Yu, Feng Dengguo, Liu Chunyong. TPM context manager and dynamic configuration management for trusted virtualization platform [J]. Wuhan University Journal of Natural Sciences, 2008, 13(5): 1-8

[67] Chen Xiaofeng, Feng Dengguo. Direct anonymous attestation based on bilinear maps [J]. Journal of Software, 2010, 21(8): 2070-2078 (in Chinese)
(陈小峰, 冯登国. 一种基于双线性映射的直接匿名证明方案[J]. 软件学报, 2010, 21(8): 2070-2078)

[68] Chen Xiaofeng, Feng Dengguo. A new direct anonymous attestation from bilinear maps [C] //Proc of The 2008 Int Symp on Trusted Computing. Los Alamitos, CA: IEEE Computer Society, 2008: 2308-2313

[69] Feng Dengguo, Xu Jing, Chen Xiaofeng. An efficient direct anonymous attestation scheme with forward security [J]. WSEAS Transas on Communications, 2009, 10(8): 1076-1085

[70] Chen Xiaofeng, Feng Dengguo. A direct anonymous attestation scheme in multi-domain environment [J]. Chinese Journal of Computers, 2008, 31(7): 1122-1130 (in Chinese)
(陈小峰, 冯登国. 一种多信任域内的直接匿名证明方案[J]. 计算机学报, 2008, 31(7): 1122-1130)

[71] Feng Dengguo, Qin Yu. A property-based attestation protocol for TCM [J]. Science in China: Series F Information Sciences, 2010, 53(3): 454-464 (in Chinese)
(冯登国, 秦宇. 一种基于TCM的属性证明协议[J]. 中国科学: F辑 信息科学, 2010, 40(2): 189-199)

[72] Qin Yu, Feng Dengguo, Xu Zhen. An anonymous property-based attestation protocol from bilinear maps [C] //Proc of Int Conf on Computational Science and Engineering. Los Alamitos, CA: IEEE Computer Society, 2009: 732-738

[73] Qin Yu, Feng Dengguo. Component property-based remote attestation [J]. Journal of Software, 2009, 20(6): 1625-1641 (in Chinese)
(秦宇, 冯登国. 基于组件属性的远程证明[J]. 软件学报, 2009, 20(6): 1625-1641)

[74] Yu Aimin, Chu Xiaobo, Feng Dengguo. Research of platform anonymous identity management based on trusted chip [J]. Chinese Journal of Computers, 2010, 33(9): 1-10 (in Chinese)
(于爱民, 初晓博, 冯登国. 基于可信芯片的终端平台匿名身份建立方法研究[J]. 计算机学报, 2010, 33(9): 1-10)

[75] Wang Dan, Feng Dengguo, Xu Zhen. An approach to data sealing based on trusted virtualization platform [J]. Journal of Computer Research and Development, 2009, 46(8): 1325-1333 (in Chinese)
(汪丹,冯登国,徐震. 基于可信虚拟平台的数据封装方案[J]. 计算机研究与发展, 2009, 46(8): 1325-1333)

[76] Li Hao, Qin Yu, Feng Dengguo. Research on virtual monotonic counters using trusted platform module [J]. Journal of Computer Research and development, 2011, 48(3): 415-422 (in Chinese)
(李昊,秦宇,冯登国. 基于可信平台模块的虚拟单调计数器研究[J]. 计算机研究与发展, 2011, 48(3): 415-422)

[77] Chu Xiaobo, Qin Yu. A distributed usage control system based on trusted computing [J]. Chinese Journal of Computers, 2010, 33(1): 93-102 (in Chinese)
(初晓博, 秦宇. 一种基于可信计算的分布式使用控制系统[J]. 计算机学报, 2010, 33(1): 93-102)

[78] Li Hao, Hu Hao. UCFS: Building a usage controlled file system with a trusted platform module [C] //Proc of the 1st Chinese Conf on Trust Computing Theory and Practice. Beijing: Tsinghua University Press, 2009: 10-23

[79] Yu Aimin, Feng Dengguo, Liu Ren. TBDRM: A TPM-based secure DRM architecture [C] //Proc of Int Conf on Computational Science and Engineering. Los Alamitos, CA: IEEE Computer Society, 2009: 671-677

[80] Hu Hao, Li Hao, Feng Dengguo. L-UCON: Towards layered access control with UCON [C] //Proc of Int Conf on Computational Science and Engineering. Los Alamitos, CA: IEEE Computer Society, 2009: 823-829

[81] Chen Xiaofeng. The formal analysis and testing of trusted platform module [J]. Chinese Journal of Computers, 2009, 32(4): 27-34 (in Chinese)
(陈小峰. 可信平台模块的形式化分析和测试[J]. 计算机学报, 2009. 32(4): 27-34)

[82] Li Hao, Hu Hao, Chen Xiaofeng. Research on compliant testing method of trusted cryptography module [J]. Chinese Journal of Computers, 2009, 32(4): 1-10 (in Chinese)
(李昊, 胡浩, 陈小峰. 可信密码模块符合性测试方法研究[J]. 计算机学报, 2009. 32(4):1-10)

[83] Chinese Association for Cryptologic Research. China Report on Advances in Cryptography, 2008 [M]. Beijing: Publishing House of Electronics Industry, 2009 (in Chinese)
(中国密码学会. 中国密码学发展报告 2008 [M]. 北京: 电子工业出版社, 2009)

[84] Shen Changxiang, Zhang huanguo, Feng Dengguo, et al. A survey of information security [J]. Science in China: Series F Information Sciences, 2007, 50(3): 273-298 (in Chinese)
(沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学: F 辑 信息科学, 2007, 37(1): 129-150)

[85] Feng Dengguo. Security protocol—Theory and practice [M]. Beijing: Tsinghua University Press, 2011 (in Chinese)
(冯登国. 安全协议——理论与实践[M]. 北京: 清华大学出版社, 2011)

Feng Dengguo, born in 1965. Professor and PhD supervisor. Senior member of China Computer Federation. His current research interests include cryptography and information security.

Qin Yu, born in 1979. PhD and assistant professor. His current research interests include information security and trusted computing(qin_yu@is.iscas.ac.cn).

Wang Dan, born in 1982. PhD and assistant professor. Her current research interests include information security and trusted computing.

Chu Xiaobo, born in 1984. PhD. His current research interests include information security and trusted computing (chuxiaobo@is.iscas.ac.cn).