信任评估与服务选择

杜瑞忠　蔡红云
梁晓艳　刘凡鸣　著

科学出版社

信任评估与服务选择

杜瑞忠　蔡红云　梁晓艳　刘凡鸣　著

科学出版社

北京

内 容 简 介

本书在简要介绍可信计算、信任评估已有研究成果的基础上，主要介绍作者在信任评估与服务选择等方面的研究成果。主要内容包括：信任评估与信任评估模型、基于个性偏好的服务选择算法、云计算环境下基于信任和个性偏好的服务选择模型、基于信任力矩的服务资源选择模型、面向社交网的个性化可信服务推荐方法、基于信誉属性的动态云资源预留方法等。

本书可以作为信息安全及相关专业研究生教材，也可供从事信息安全与电子商务相关研究和开发的人员阅读参考。

图书在版编目 (CIP) 数据

信任评估与服务选择 / 杜瑞忠等著. —北京：科学出版社，2017.11

ISBN 978-7-03-054891-7

Ⅰ. ①信… Ⅱ. ①杜… 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（2017）第 255976 号

责任编辑：陈 静 霍明亮 / 责任校对：郭瑞芝

责任印制：张 倩 / 封面设计：迷底书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 11 月第 一 版 开本：720×1 000 1/16

2017 年 11 月第一次印刷 印张：13 1/4

字数：252 000

定价：78.00 元

（如有印装质量问题，我社负责调换）

前　言

网络空间已经成为继陆、海、空、天之后的第五大主权领域空间。可信计算是我国网络空间安全的核心关键技术。可信计算技术研究的出发点是要解决传统主机执行程序可被随意修改、系统完整性可被破坏、恶意代码可被植入运行、系统漏洞可被随意利用、用户权限可被越权、密码信息可被窃取等一系列安全问题。我国以及国家可信计算组织（Trusted Computing Group，TCG）提出可信计算技术的核心特征概括为：基于可信硬件设备构建可信根，从计算平台启动开始，一级度量一级，一级信任一级，建立从底层软硬件到应用程序的信任链。

我国在可信计算领域发展具有自己的特色，起步不晚，水平不低，成果可喜，已经走在了世界的前列。

自2000年起，我们研究小组在分布式系统可靠性、信息安全等领域开展了一系列研究和开发工作。2000年，为提高分布计算系统的性能，我们在河北省自然科学基金项目资助下，在代理技术和分布式冗余服务可靠性、可用性等相关领域取得了一系列研究成果。2002年，在河北省科技转化基金项目“高可靠、可扩展分布式数据库服务器”的资助下，研制成功了高可用、可扩展分布式数据库服务器YF-Ⅰ和YF-Ⅱ，并在“医政信息管理系统”“教务系统”“邮件服务器系统”中得到了实际应用，取得了显著的经济和社会效益。在国家高技术研究发展计划（863计划）子课题、河北省自然科学基金项目及河北省教育厅自然科学基金重点项目的资助下，对蜜罐、认证、入侵检测、攻击预警等技术展开研究，相应成果已成功地应用到河北省农业信息网、国际合作项目“基于流媒体技术的安全电子商务平台”等系统中，有效地保障了系统的安全性。

分布式网络具有开放性、动态性及资源共享等特性，面对海量的资源和服务，由于存在大量欺诈行为及不可靠服务质量，用户在增加选择机会的同时也面临着如何识别和选择一个既安全、可靠又满足其个性偏好的资源或服务问题。当前一个有效的解决方法是利用信任评估系统，通过收集、分析实体历史行为信息，预测在未来的交易中其可能的行为。通过信任评估系统，选择信任值高的实体进行交易，降低双方由于缺乏了解而盲目交易可能造成的损失及交易失败的风险，提高交易成功率。

从2008年起，在国家自然科学基金、河北省杰出青年基金、河北省自然科学重点基金等项目的支持下，遵循“可信≈可靠+安全”的理念，针对可信计算、信任链传递、可信管理、信任评估、可信服务推荐、可信服务选择等领域展开研究，取

得了一些成果并为国家培养了几十名可信计算方向的研究生。

本书是我们研究小组十年来在信任管理、信任评估及服务选择研究方面的阶段成果总结，里面很多思想方法是在田俊峰教授指导和帮助下，由作者及团队部分研究生在完成科研项目研究和学位论文的过程中产生的，这些成果的产生得益于田俊峰教授的指导及研究生创新性研究和勤奋努力，在此对他们表示衷心的感谢。

全书共 9 章，由杜瑞忠、蔡红云、梁晓艳、刘凡鸣等撰写，全书由杜瑞忠统稿和审校。

感谢曾经参加或正在参加“可信计算技术”讨论班的所有老师和研究生，他们的建议和部分学生的论文充实了本书的内容。

本书的部分研究内容得到了国家自然科学基金项目（61170254，60873203，61379116）、河北省自然科学基金重点项目（F2016201244）、河北省高等学校科学技术研究项目（ZD2016043）、河北省物联网数据采集与处理工程技术研究中心开放课题和河北大学科研创新团队培育与扶持计划（2016 年“一省一校”专项经费）资助，特此致谢！

由于作者水平所限，书中难免会有不足之处，恳请读者批评指正。

作　者

2017 年 6 月

目　录

第1章 可信计算

大多数安全隐患来自微型计算机（简称微机）终端，因此必须提高微机的安全性。对于最常用的微机，只有对芯片、主板等硬件和基本输入输出系统（Basic Input Output System，BIOS）、操作系统（Operating System，OS）等底层软件综合采取措施，才能有效地提高安全性。基于这一思想，催生了可信计算技术。可信计算是一种信息系统安全新技术，其思想来源于人类社会，是把人类社会的管理经验用于计算机信息系统与网络空间，以确保计算机信息系统和网络空间的安全可信。

本章主要介绍可信计算的概念、主要技术、可信网络连接和可信计算的应用及未来发展趋势。

1.1 可信计算概述

据统计，80%的信息安全事件是内部人员或者内外勾结所为，其中很多问题都是由计算机体系结构存在安全隐患和操作系统的不安全引起的。沈昌祥院士[1]指出：

（1）主要由传统的防火墙、入侵监测和病毒防范构成的信息安全系统，是以防外为重点，与目前信息安全主要威胁源自内部的实际状况不相符。

（2）从组成信息系统的服务器、网络、终端三个层面上来看，现有的保护手段是逐层递减的。人们往往把过多的注意力放在对服务器和网络设备的保护上，而忽略了对终端的保护。

（3）恶意攻击手段变化多端，而传统的方法是采取封堵的办法。例如，在网络层设防，在外围对非法用户和越权访问进行封堵。而封堵的办法是捕捉黑客攻击和病毒入侵的特征信息，其特征是已发生过的滞后信息，不能科学预测未来的攻击和入侵。

为了解决计算机和网络结构上的安全问题，从根本上提高其安全性，必须从芯片、硬件结构和操作系统等方面综合采取措施，由此产生可信计算的基本思想，其目的是在计算和通信系统中广泛使用基于硬件安全模块的可信计算平台，以提高整体的安全性。

硬件系统的安全和操作系统的安全是信息系统安全的基础，密码、网络安全等是关键技术。只有从信息系统硬件和软件的底层采取安全措施，才能有效地确保信息系统的安全，这促进了可信计算的迅速发展。

可信计算的基本思想[2,3]是在计算机系统中首先建立一个信任根，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，一级测量认证一级，一级信任一级，把信任关系扩大到整个计算机系统，从而确保计算机系统的可信。

1.1.1　可信计算的发展

可信计算的出现最早可以追溯到20世纪80年代。1983年美国国防部所属的国家计算机安全中心为适应军事计算机的保密需要，在20世纪70年代的理论研究成果“计算机保密模型”的基础上，制定并出版了《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria，TCSEC)[4]，在TCSEC中第一次提出可信计算机和可信计算基(Trusted Computing Base，TCB)的概念，并把TCB作为系统安全的基础。随后，作为对TCSEC的补充，美国国防部分别在1987年和1991年相继推出了可信网络解释(Trusted Network Interpretation，TNI)[5]和可信数据库解释(Trusted Database Interpretation，TDI)[6]。由于可信计算机评价准则系列是在早期BLP(Bell-LaPadula)模型[7]的基础上提出的，所以具有一定的局限性。其主要考虑了信息的保密性，缺乏完整性、真实性控制，强调了系统安全性，却没有给出达到这种安全性的系统结构和技术路线。

1997年，Arbaugh等提出并实现了一种计算机安全引导架构AEGIS[8]，其中已经体现出“信任传递”的概念。AEGIS基于IBM PC(Personal Computer)的传统BIOS，采用认证的方法保障BIOS的完整性。计算机从启动的过程开始，由前一个程序度量后一个程序的完整性，只有在完整性通过验证后，才把控制权交给后一个程序，如此反复直到操作系统启动，这种硬件保护软件机制的思想促进了可信计算的发展。

为了解决个人计算机结构上的安全问题，并从底层入手提高其可信性，英特尔(Intel)、微软(Microsoft)、IBM、惠普(HP)、COMPAQ等著名的信息技术企业在1999年10月共同发起并成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)。TCPA定义了具有安全存储和加密功能的可信平台模块(Trusted Platform Module，TPM)，并于2001年1月发布了基于硬件系统的“可信计算平台规范”(V1.0)。TCPA的成立标志着可信计算高潮阶段的出现。2003年3月，TCPA中的AMD、HP、IBM、Intel和Microsoft对外宣布将TCPA重新改组，更名为可信计算组织(Trusted Computing Group，TCG)[9-11]，其目的是在计算和通信系统中广泛使用基于硬件安全模块的可信计算平台，以提高整体的安全性，扩展可信范围。

TCG的出现标志着可信计算技术和应用领域的进一步扩大。TCG是一个非营利组织，旨在研究制定可信计算的工业标准。TCPA和TCG已经制定了关于可信计算平台、可信存储和可信网络连接等一系列技术规范[12,13]，还在不断对这些技术标准规范进行修订、完善和版本升级。部分规范包括可信PC规范、可信平台模块规范、可信软件栈(TCG Software Stack，TSS)规范、可信服务器规范、可信网络连接

（Trusted Network Connection，TNC）规范、可信手机模块规范等。

在TCG规范的指导下，许多芯片厂商都推出了自己的可信平台模块芯片，大多数PC都配备了TPM芯片。TPM的版本经历了TPM 1.0、TPM 1.1、TPM 1.1b、TPM 1.2、TPM 2.0的发展。Microsoft推出的Windows Vista、Windows 7和Windows 8操作系统都支持可信计算，这些充分地说明可信计算产品已经走向实际应用。

2016年6月，微软向OEM（Original Equipment Manufacturer）厂商发布了最新的Windows 10最低配置要求，增加了2GB以上内存和配备TPM 2.0加密芯片，通过TPM 2.0加密来有效地提高系统安全性，为Windows Hello验证功能提供支持，并保证软件安全方案难以攻破。今后不配备TPM 2.0加密芯片的Windows 10 PC、智能手机和平板硬件产品都将被视为“非Windows 10兼容”。TPM 2.0已成为国际标准化组织（International Organization for Standardization，ISO）和国际电工委员会（International Electrotechnical Commission，IEC）认定的国际标准。

TCG可信计算的意义包括以下几部分。

（1）首次提出可信计算平台的概念，并把这一概念具体化到服务器、微机、掌上电脑（Personal Digital Assistant，PDA）和移动计算设备，而且具体给出了可信计算平台的体系结构和技术路线。

（2）不仅考虑了信息的秘密性，还强调了信息的真实性和完整性。

（3）更加产业化和更具有广泛性，国际上已有100多家信息技术行业的著名公司加入TCG。

2015年6月，国际标准化组织和国际电工委员会信息技术标准联合技术委员会批准国际可信计算组织的可信平台模块2.0规范库（TPM 2.0, Trusted Platform Module 2.0）作为ISO/IEC 11889: 2015发布。

可信平台模块2.0规范库特点包括以下几方面。

（1）密码算法应用灵活性，新框架支持已有和未来的算法。

（2）密码算法失效或生命周期结束不需要重新编写标准规范。

（3）满足各个国家或地区对于密码算法的多样性需求，支持中国SM2（部分）/SM3/SM4密码算法。

（4）满足不同安全级别对密码算法的应用需求。

（5）增加虚拟化支持，为云计算提供应用基础。

（6）增加用户授权管理模式，简化应用，提高易用性。

（7）学习中国可信密码模块（Trusted Cryptographic Module，TCM）技术广泛使用对称密码算法，提高应用性能。

（8）去除TPM 1.2中无用或者实现代价高的安全协议。

（9）面向嵌入式应用，增加多密钥树管理结构。

（10）增加安全时钟适应更多安全应用场景。

TPM 2.0 与 TPM 1.2 安全协议不兼容，TPM 2.0 对于产业是一个新的开始。

TPM 2.0 规范库中对密码算法应用约定如下。

（1）规范定义一个 TPM 2.0 的实现实体包含密码算法子系统。

（2）规范不要求实施特定的密码算法集。

（3）一个 TPM 2.0 实现实例必须包含至少一个对称密码算法，一个非对称密码算法和一个哈希密码算法。

目前已支持的中国密码算法包括以下几种。

（1）《GM/T 0002—2012 SM4 分组密码算法》。

（2）《GM/T 0003—2012 SM2 椭圆曲线公钥密码算法》。

（3）《GM/T 0004—2012 SM3 密码杂凑算法》。

国际可信计算产业应用发展趋势有以下几方面。

（1）产业快速向 TPM 2.0 应用迁移。

① Intel Skylake 平台全面支持 TPM 2.0 应用。

② Windows 10 从安全启动、Bitlockor 整盘数据加密、虚拟智能卡、身份认证等方面加强支持 TPM 2.0 应用。

③ 开源项目快速支持 TPM 2.0，如 Linux Kernel 4.0 支持 TPM 2.0 驱动、IBM 发布开源 TSS 2.0 中间件。

（2）云终端、网络设备、智能手机、云服务、智能汽车等多领域应用逐步形成。

TCG 2020 年愿景："TCG Enabled"的国际标准在全球范围成为创建系统信任的技术基础；使用范围从复杂的大型计算平台到小型专用设备，从传统的信息技术（Information Technology，IT）到工厂车间，再到我们日常生活的各种设备。

可信计算已成为全球计算机安全技术发展趋势。我国在可信计算研究方面起步不晚，水平不低，成果喜人[2,3]，具体包括以下几方面。

1）产品开发方面

2004 年 6 月，瑞达信息安全产业股份有限公司（简称瑞达公司）推出了国内首款自主研发的具有 TPM 功能的 SQY-14 嵌入密码型计算机，并于同年 10 月通过了国家商用密码管理办公室（简称国家密码管理局）主持的技术鉴定。该可信安全计算机基于 SSP02 芯片，采用瑞达嵌入式安全模块（Embedded Security Module，ESM），运用硬件的系统底层设计，结合瑞达安全增强的 Linux 操作系统，极大地提升了 PC 的安全性。主要安全功能包括平台身份识别、平台完整性校验和芯片级的安全。2005 年 4 月联想推出了"恒智"安全芯片，成为继 ATLEM 之后全球第二个符合 TPM 1.2 标准安全芯片的厂商。同年，北京兆日科技有限责任公司（简称兆日科技）基于可信计算技术的 PC 安全芯片的安全产品也正式推出，这些产品也通过了国家密码管理局的鉴定。此后不久，采用联想"恒智"安全芯片的联想开天 M400S 以及采用兆日 TPM 安全芯片（SSX35）的清华同方超翔 S4800、长城世恒 A 和世恒 S 系列安全 PC

产品纷纷面世。产品应用方面，在某省涉密网的设计中已经采用了可信计算平台，另外，在金融、电信、军队、公安、电子政务领域也开始采用可信计算机来提高信息安全的整体水平。2008 年，兆日科技的可信计算机密码模块安全芯片和可信计算密码支撑平台、深圳市中兴集成电路设计有限责任公司的可信计算密码支撑平台通过了国家密码管理局的认证。武汉大学研制出我国第一款可信 PDA 和第一个可信计算平台测评软件系统。2009 年瑞达公司的可信计算机密码模块安全芯片通过了国家密码管理局的认证。

2008 年 4 月底，中国可信计算联盟（Chinese Trusted Computing Union，CTCU）在国家信息中心成立，现已有 20 家正式成员，包含计算机厂商、信息安全厂商和一些应用厂商，也包含国家的科研院所。2014 年 4 月 16 日，中关村可信计算产业联盟正式成立，联盟会员单位已发展到 200 多家，涉及国内可信计算产业链的各个环节，覆盖了“产学研用”各界。中国可信计算联盟和中关村可信计算产业联盟的成立，标志着我国可信计算由理论逐步转化为产业，并转入实质性的实现阶段。

2）标准研究方面

为推动可信计算标准工作，2005 年 1 月全国信息安全标准化技术委员会在北京成立了 TC260 可信计算工作小组（WG1），这体现了国家对可信计算标准的高度重视。我国已经筹建了中国可信计算平台联盟（China Trusted Computing Platform，CTCP）的可信计算组织，该组织制定的规范与 TCG 的标准保持大部分兼容，只在涉及国家安全的极少部分有一些不同；另外，从国家层面来看，2005 年出台的国家“十一五”规划和 863 计划中，已将可信计算列入重点支持项目，并有较大规模的投入与扶植。2016 年 3 月，中关村可信计算产业联盟面向会员发布《可信计算体系结构规范 v1.0》、《可信平台控制模块规范 v1.0》、《可信软件基规范 v1.0》和《可信服务器平台规范 v1.0》。此外，《可信存储系统架构规范 v1.0》和《可信计算机评估规范 v1.0》也将于近期面向会员发布。

3）革命性创新方面

可信计算的发展经历了几个阶段。最初的可信 1.0 来自计算机的可靠性，主要以故障排除和冗余备份为手段，是基于容错方法的安全防护措施。可信 2.0 以 TCG 出台的 TPM 1.0 为标志，主要以硬件芯片作为信任根，以可信度量、可信存储、可信报告等为手段，实现计算机的单机保护。不足之处在于：未从计算机体系结构层面考虑安全问题，很难实现主动防御。

我国的可信计算技术已经发展到了 3.0 阶段的“主动防御体系”，确保全程可测可控、不被干扰，即防御与运算并行的“主动免疫计算模式”。

可信计算 3.0 革命性的创新包括以下几方面。

（1）全新的可信计算体系结构。相对于国外可信计算被动调用的外挂式体系结构，中国可信计算革命性地开创了自主密码为基础的控制芯片为主、双融主板为平

台、可信软件为核心、可信连接为纽带、策略管控成体系、安全可信保应用的可信计算体系结构。

（2）跨越了国际可信计算组织可信计算的局限性。其中包含密码体制的局限性，TCG 原版只采用了公钥密码算法 RSA，杂凑算法只支持 SHA-1 系列，回避了对称密码。由此导致密钥管理、密钥迁移和授权协议设计复杂化，也直接威胁着密码的安全。TPM 2.0 采用了我国对称与非对称结合的密码体制，并申报成了国际标准；此外，TCG 采用外挂式结构，未从计算机体系结构上作变更，把可信平台模块作为外部设备挂接在外总线上。

（3）创建主动免疫体系结构。主动免疫是中国可信计算革命性创新的集中体现。在双系统体系架构下，采用自主创新的对称和非对称相结合的密码体制，通过可信平台控制模块（Trusted Platform Control Model，TPCM）植入可信根（root of trust），在 TCM 基础上加以信任根控制功能，实现密码与控制相结合，将可信平台控制模块设计为可信计算控制节点，实现了 TPCM 对整个平台的主动控制。

可信 3.0 已经形成了自主创新的体系，并在很多领域开展了规模应用。我国研究人员经过长期攻关，取得了巨大的创新成果，包括：平台密码方案创新，提出了可信计算密码模块，采用 SM 系列国产密码算法，并自主设计了双数字证书认证结构；提出了可信平台控制模型，TPCM 作为自主可控的可信节点植入可信根，先于中央处理器（Central Processing Unit，CPU）启动并对基本输入输出系统进行验证；将可信度量节点内置于可信平台主板中，构成了宿主机 CPU 加可信平台控制模块的双节点，实现信任链在“加电第一时刻”开始建立；提出可信基础支撑软件框架，采用宿主软件系统+可信软件基的双系统体系结构；提出基于三层三元对等的可信连接框架，提高了网络连接的整体可信性、安全性和可管理性。

综上，可信 3.0 的创新点可概括为：“自主密码为基础，可控芯片为支柱，双融主板为平台，可信软件为核心，对等网络为纽带，生态应用成体系”。同时经过多年技术攻关和应用示范，可信 3.0 已具备了产业化条件[14]。

1.1.2　可信计算的概念

1. 可信计算的定义

可信计算的首要问题是要回答什么是可信，目前，关于“可信”尚未形成统一的定义，不同的专家和不同的组织机构有不同的解释，使用比较多的主要包括以下几种。

（1）TCG 用实体行为的预期性来定义“可信”：如果一个实体的行为是以预期的方式符合预期的目标，则该实体是可信的[15]。

（2）ISO/IEC 15408 标准定义“可信”为：参与计算的组件、操作或过程在任意条件下是可预测的，并能够抵御病毒和物理干扰[16]。

（3）IEEE CS 可信计算技术委员会（IEEE Computer Society Technical Committee