信息安全技术丛书

可信计算与信任管理

田俊峰　杜瑞忠
蔡红云　李　珍　著

科学出版社

内 容 简 介

本书在简要介绍可信计算和信任管理的基本概念、国内外学者的部分研究成果的基础上，秉承“可信≈可靠+安全”观点，主要介绍了作者在可信计算特别是信任管理方面多年的研究成果。主要内容包括：分布式系统的可靠性、信任链技术、可信软件栈、可信评测技术、信任网络构建、基于主观逻辑的信任模型、基于场论的信任模型、软件动态行为可信技术及其应用、可信云计算技术等。

本书可以作为信息安全及相关专业高年级本科生和研究生教材，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

可信计算与信任管理/[illegible]等著. —北京：科学出版社，2014.9
(信息安全技术丛书)
ISBN 978-7-03-041[illegible]-3

Ⅰ. ①可… Ⅱ. ①田… 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(2014)第 202709 号

策划编辑：陈 静 / 责任编辑：陈 静 王迎春
责任校对：胡小洁 / 责任印制：肖 兴 / 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

*

2014 年 9 月第 一 版 开本：720×1 000 1/16
2014 年 9 月第一次印刷 印张：24 1/4
字数：490 000

定价：99.00 元

（如有印装质量问题，我社负责调换）

信息安全技术丛书

可信计算与信任管理

田俊峰　杜瑞忠　蔡红云　李　珍　著

科学出版社

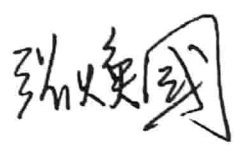
北　京

成。2012 年 6 月，武汉大学、Intel 公司、华为公司、国民技术公司、中标软件公司、道里云公司、百敖公司联合发起成立了中国可信云计算社区，旨在以自愿和开放的形式开发采用中国商用密码的可信云计算系统，促进我国可信云计算技术的产业化。经过一年多的发展，参加这一社区的单位又增加了很多，而且华为公司的可信云服务器已实现了产业化。目前，可信计算的应用在我国正在逐步推广普及。

安全可靠是用户对可信计算的基本要求，我们认为“可信≈可靠+安全”，安全与容错相结合是可信计算发展的技术路线。河北大学田俊峰教授领导的科研小组前期一直从事系统可靠性、可用性及信息安全理论研究和实践成果推广。在网络与信息安全领域，通过研究蜜罐、认证、入侵检测、攻击预警等技术，设计并实现了一个分布式网络安全监测与攻击预警模型，相关研究成果也得到了成功应用。

在前期系统可靠性、可用性及信息安全理论研究和实践应用的基础上，该研究小组成为我国在可信计算领域开展研究工作较早的单位之一，经过多年的积累，已经在可信计算领域取得了一些有影响的科研成果。2012 年，我作为评审专家参加了该小组研发的可信软件开发平台的鉴定工作，该成果已在军队、地方相关部门得到了很好的应用。今天，看到他们把自己的科研成果整理成学术专著，我向田俊峰教授以及他的研究小组表示祝贺，并预祝他们在今后的研究工作中取得更杰出的成果。

可信计算技术作为信息安全领域的一项新技术，还有许多理论和技术问题有待人们研究和解决，当前以云计算、物联网、大数据为代表的一批新兴信息技术与产业的出现为可信计算应用拓展了新空间，将可信计算技术与它们相结合，必将产生更多更好的成果，可信计算技术将大有作为。



2014 年 3 月

序

随着信息化的发展，信息安全保障能力已成为一个国家综合国力的重要组成部分，信息安全和政治安全、经济安全、文化安全并列成为国家安全的重要组成部分，成为影响国家安全、社会稳定和经济发展的决定性因素之一，因此必须采取措施确保我国的信息安全。

根据信息论的基本原理，要确保信息安全，应该从信息系统安全角度入手，而信息系统的硬件安全和操作系统安全是信息系统安全的基础。因此，只有从信息系统硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全，这一技术思想催生了可信计算的产生和发展。

1983 年，美国国防部制定了《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria，TCSEC)，并提出了可信计算机的概念。1999 年，IBM、Intel、HP、Microsoft 等国际知名企业发起成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)，并在 2003 年改名为可信计算组织(Trusted Computing Group，TCG)。TCPA 和 TCG 的出现掀起了可信计算研究的新高潮。

我国在可信计算领域起步不晚、水平不低、成果可喜，已经站在国际可信计算领域的前列。

2003 年，武汉大学和武汉瑞达信息安全产业股份有限公司(简称瑞达公司)合作研制出我国第一个可信计算平台模块和第一个可信计算平台，并通过了国家商用密码管理办公室(简称国家密码管理局)的安全审查，于 2004 年 10 月通过技术鉴定，被国家科学技术部等四部委联合认定为国家级重点新产品，并得到了实际应用。2006 年这一成果获国家密码科技进步二等奖。

2004 年 10 月，第一届中国可信计算与信息安全学术会议在武汉大学召开。2006 年 10 月，第二届中国可信计算与信息安全学术会议在河北大学召开，会议收到学术论文 1200 余篇，400 多位代表参加了会议。当前，这一学术会议已成为我国可信计算和信息安全领域的一个品牌会议，得到了广大可信计算和信息安全同行的认可。2007 年我国国家自然科学基金启动了可信软件重大研究专项。2007 年 12 月，联想、清华同方、中兴集成电路、方正等 12 家个人计算机、软件、芯片企业联合举办了打造中国信息安全 DNA——中国自主可信计算产品联合发布会。2008 年中国可信计算联盟(Chinese Trusted Computing Union，CTCU)成立。同年，全球首款符合可信密码模块(Trusted Cryptography Module，TCM)规范的芯片诞生，这标志着覆盖安全芯片、可信计算机、可信操作系统、安全软件的“安全 PC”产业链已经在我国初步形

级信任一级，把这种信任关系扩展到整个计算机系统，从而确保整个计算机系统的可信。当前可信计算的研究现状是理论上不成熟且滞后于技术。

从2005年开始，我们开设了“可信计算技术”讨论班，在前期系统可靠性、可用性及信息安全理论研究和实践成果基础上，秉承“可信≈可靠+安全”理念，对可信计算特别是信任管理理论进行了探讨和研究，我们研究小组成为我国在可信计算领域开展研究工作较早的单位之一。2006年我们成功组织了第二届中国可信计算与信息安全学术会议，得到了同行的认可。

通过开展可信计算技术研究，我们在可信计算领域取得了一些成果，本书是我们研究小组十年来在可信计算与信任管理研究方面的阶段成果总结，里面很多思想方法是在我的指导下，由我的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他们的创新性研究和勤奋努力，在此对他们表示衷心的感谢。

全书共分两篇12章，由田俊峰、杜瑞忠、蔡红云、李珍、何欣枫等撰写，全书由田俊峰统稿和审校。

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。

在可信计算与信任管理理论研究过程中，我们得到了武汉大学的张焕国教授、中国科学院计算技术研究所的张玉清教授、北京航空航天大学的刘建伟教授等众多专家的支持和帮助，在此向他们表示衷心的感谢。

本书的部分研究内容得到了国家自然科学基金项目(编号：61170254、60873203)、河北省杰出青年科学基金项目(编号：F2010000317)、河北省自然科学基金项目(编号：F2012201145)、河北省高等学校科学技术研究重点项目(编号：ZH2012029)和河北省高校学术著作出版基金的资助，特此致谢。

由于作者学识和水平所限，书中难免会有不足之处，恳请读者批评指正。

作　者

2014年1月

前　言

信息技术的迅速发展把人类推进信息革命的历史潮流，信息革命成为人类第三次最伟大的生产力革命，信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。信息已成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家重要的基础设施。

任何事物都具有两面性，信息技术也不例外。一方面，信息技术的发展使人类生活更便捷；另一方面，危害信息安全的事件也不断发生，如敌对势力的破坏、恶意软件的入侵、黑客攻击、利用计算机犯罪等，这些事件对信息安全构成了极大的威胁。因此，信息的获取、存储、传输、处理过程中的安全保障能力已成为一个国家综合国力和经济竞争力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一，信息安全问题也由此成为世人关注的社会问题和信息科学与技术领域的热点研究问题。

由信息论原理可知，应该从信息系统安全角度入手，以确保信息安全，而信息系统安全的基础体现为信息系统的硬件安全和操作系统安全。因此，为了比较有效地确保信息系统的安全，必须从信息系统硬件和软件的底层做起，从整体上采取措施，由此催生了可信计算的产生和发展。

可信计算组织从实体行为角度对可信计算进行了定义：如果一个实体的行为总是以预期的方式达到预期目标，则称其为可信的。可信计算的总目标是提高计算机系统的可信性。沈昌祥院士和张焕国教授将可信解释为“可信≈可靠+安全”，可信计算机系统是能够提供可信计算服务的计算机系统，它能提供系统的可靠性、可用性、主体行为与信息的安全性。

在2000—2005年，我们研究小组一直从事系统可靠性、可用性及信息安全理论研究和实践成果推广工作。为了提高数据库服务器的可靠性和可用性，在2001年，我们成功研制了具有自主知识产权的高可用、可扩展分布式数据库服务器YF-I和YF-II，并得到了实际应用，《科技时报》、《河北日报》等多家媒体对此进行了报道，2002年该成果获河北省科技进步三等奖。在网络与信息安全领域，通过研究蜜罐、认证、入侵检测、攻击预警等技术，设计并实现了一个分布式网络安全监测与攻击预警模型，相关研究成果也成功应用到政务系统及相关国际合作项目中。

可信计算的基本思想是：在计算机系统中，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、操作系统，再到应用，一级度量认证一级，一

目　录

第二篇　信 任 管 理

第一篇　信息安全与可信计算

第 1 章　信息安全概论

国家安全以国民安全为核心，以领土、政治、军事、经济等多方面安全为保障条件。随着信息技术(Information Technology，IT)的广泛应用，信息化已渗透到国民生活的各个领域，信息安全问题已成为影响国民安全的重要内容之一。本章主要介绍信息安全的现状、信息安全问题存在的原因、信息安全的内涵及其发展趋势等方面的内容。

1.1　信息安全现状

信息技术的迅速发展把人类推进到信息革命的历史潮流，信息革命成为人类第三次最伟大的生产力革命，信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。信息已成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家重要的基础设施。

任何事物都具有两面性，一方面信息技术的发展给人类带来方便；另一方面危害信息安全的事件不断发生，如敌对势力的破坏、恶意软件的入侵、黑客攻击、利用计算机犯罪等，对信息安全构成了极大的威胁。

好莱坞电影《国家公敌》中有这样一个情节：网民的信息被人完全操控，然而这样骇人的场景竟成为现实——随着“棱镜”事件的充分暴露，世界各地的网民绝不会想到他们在使用谷歌、Facebook、苹果等知名公司的网络产品进行社交、办公或存储信息时，他们屏幕的背后正隐藏着美国情报部门的身影。换句话说，人们在网上的一举一动都可能被美国情报部门看在“眼”里，记在“芯”上。

如果说“棱镜”计划还只是信息窃取事件，那么之前伊朗核设施被“震网”病毒破坏已经不再是窃密，而是毁坏基础设施。对于我国，信息安全形势的严峻性更在于我国对外国品牌的电子产品、信息技术产品过分依赖，例如，CPU 芯片、计算机操作系统、数据库、路由器等核心技术，在涉及政府、海关、邮政、金融、铁路、民航、医疗、军警等国家关键信息基础设施的建设中，频频出现美国“八大金刚”(思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软)的影子，导致我国信息安全失去了自主可控的基础，这无疑对我国信息安全构成了潜在威胁。

“棱镜”事件表明，那些提供信息技术设备与服务的美国公司往往会按照美国情报部门的要求行事。要想使用它们而又不被此类计划监控，恐怕只能是痴心妄想。信息技术设备应能自主可控，在此基础上，再努力加强信息安全防护，这样才有可能保障国家信息安全。

因此，信息的获取、存储、传输、处理和安全保障能力已成为一个国家综合国力和经济竞争力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一。

为了保障我国的信息安全和信息化建设，2014 年 2 月我国成立了中央网络安全和信息化领导小组，中共中央总书记、国家主席、中央军委主席习近平任组长。习近平指出：没有网络安全就没有国家安全，没有信息化就没有现代化，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局、统筹各方、创新发展，努力把我国建设成为网络强国。

信息安全已成为世人关注的社会问题和信息科学与技术领域的热点研究问题。信息安全是信息时代永恒的需求，是确保人们赖以生存的社会和信息空间和谐繁荣的重要因素之一。

1.2　信息安全问题存在的原因

信息安全问题如此严重，从技术角度分析主要包括以下几方面。

1. 个人计算机的安全结构设计简单[1-2]

在 20 世纪 70 年代，随着集成电路技术的发展，出现了微型计算机(简称微机)，随后个人计算机(Personal Computer，PC)逐渐普及。由于定位为个人计算机，而不是公用计算机，所以在设计时为了降低成本舍去了很多安全机制，如存储器的隔离保护机制、程序安全保护机制等。其中，程序的执行可以不经过认证，程序和系统区域的数据可以被随意修改，这样就可能导致病毒、木马、蠕虫等恶意代码的泛滥。随着网络技术的发展和应用，个人计算机通过网络连接而变为网络中的一个组成部分，在连接上突破了地理位置的限制，信息的交互和处理扩大到整个网络，面对这种环境，个人计算机的安全防御能力就显得比较弱。

2. 互联网的开放性

互联网是开放式体系结构，这种特性加速了互联网的发展，但同时因缺少整体的规划，使得当前很多协议的制定是为了弥补之前的设计漏洞、蓝图的缺失带来的计算机网络基础设施和协议中的各种风险。