“十一五”国家重点图书

可信计算

TRUSTED COMPUTING

张焕国　赵　波　等著

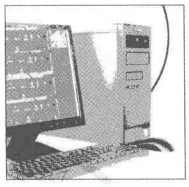
WUHAN UNIVERSITY PRESS
武汉大学出版社

“十一五”国家重点图书

可信计算

TRUSTED COMPUTING

张焕国 赵 波 等著



WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

可信计算/张焕国,赵波等著. —武汉：武汉大学出版社,2011.8
“十一五”国家重点图书
ISBN 978-7-307-09046-0

Ⅰ.演… Ⅱ.①张… ②赵…[等] Ⅲ.电子计算机—安全技术
Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2011)第 153140 号

责任编辑:刘 阳 责任校对:黄添生 版式设计:王 晨

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)
印刷:武汉中远印务有限公司
开本:787×1092 1/16 印张:30.75 字数:649 千字 插页:3
版次:2011 年 8 月第 1 版 2011 年 8 月第 1 次印刷
ISBN 978-7-307-09046-0/TP·405 定价:65.00 元

序

随着社会的信息化，信息安全保障能力成为一个国家综合国力的重要组成部分，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，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可知，信息不能脱离它的载体而孤立存在，因此我们应当从信息系统安全角度来确保信息安全。信息系统的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、网络安全等技术是关键技术。只有从信息系统的硬件和软件的底层作起，从整体上采取措施，才能比较有效地确保信息系统的安全。正是这一技术思想推动了可信计算的产生和发展。

1983 年美国国防部制定了世界上第一个《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria，TCSEC)。在 TCSEC 中第一次提出可信计算机(Trusted Computer)的概念。之后，美国国防部又相继推出了可信网络解释(Trusted Network Interpretation，TNI)和可信数据库解释(Trusted Database Interpretation，TDI)。从而形成了最早的一套可信计算技术文件。

1999 年底，IBM、Intel、HP、微软等著名 IT 企业发起成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)，2003 年 TCPA 改组为可信计算组织 TCG(Trusted Computing Group，TCG)。TCPA 和 TCG 的出现形成了可信计算的新高潮。欧洲也在 2006 年启动了开放式可信计算(Open Trusted Computing)的研究计划。

我国在可信计算领域，起步不晚，并且取得了许多可喜的成绩。

2000 年 6 月武汉瑞达公司和武汉大学合作，开始研制安全计算机。2003 年研制出我国第一款可信计算平台模块和第一款可信计算平台，2003 年 7 月 15 日通过国家密码管理局的安全审查。2004 年 10 月通过国家密码管理局主持的技术鉴定。这一新产品被国家科技部等四部委联合认定为“国家级重点新产品”，并得到实际应用。2006 年这一成果获国家“密码科技进步二等奖”。

2004 年 6 月由瑞达公司和武汉大学联合在武汉大学召开中国首届可信计算平台(TCP)论坛。同年 10 月，在武汉大学召开了“第一届中国可信计算与信息安全学术会议”。

2005 年，联想公司、兆日公司的 TPM 芯片和联想公司的可信计算机也相继研制成功。这些产品也都通过了国家密码管理局的认证。

从2006年开始我国进入制定可信计算规范和标准的阶段，在国家密码管理局和国家信息安全标准化委员会的主持下，我国制定了一系列的可信计算规范与标准。我国成为除TCG之外唯一拥有自主可信计算规范与标准的国家。

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。

2008年中国可信计算联盟(CTCU)成立。

从2007年开始，符合我国技术规范的可信计算产品相继出现，可信计算的应用进一步扩大。

至此，我国的可信计算技术与产业取得了辉煌的成绩，我国已经站在国际可信计算领域的前列。

武汉大学张焕国教授的研究小组在可信计算领域作出了许多重要的贡献。他们与瑞达公司合作研制出我国第一款可信计算平台模块和第一款可信计算平台。他们发起组织了我国第一届中国可信计算与信息安全学术会议。这一会议得到了广大可信计算和信息安全同行的厚爱，已经成为我国学术会议中的一个品牌会议。他们参加了我国一系列的可信计算规范和标准的制定工作，并在其中发挥了骨干的作用。在国家863计划项目的支持下，他们研制出我国第一款可信PDA和可信计算平台测评系统。此外，他们还与国内外企业合作，进行了可信计算应用的研发工作，取得了国内外同行高度认可的成果。他们为国家培养了几十名可信计算方向的博士和硕士研究生，其中许多人已经成为我国可信计算领域的优秀人才。

本书集中介绍了张焕国教授的研究小组十年来在可信计算领域的研究成果。本书的出版将会推进可信计算理论与技术的交流，促进可信计算的深入研究。

2000年张焕国教授与瑞达公司合作向国家密码管理局申请开展安全计算机的研究，我支持了这一申请。作为评审专家，我参加了这一研究过程中的多次评审，亲身见证了这一研究从申请到成果鉴定的全过程。此外，我还亲身见证了他们积极参加我国一系列的可信计算规范和标准的制定工作并在其中发挥了骨干的作用。今天我又看到他们把自己的科研成果写成学术专著《可信计算》，我由衷地感到高兴。我向张焕国教授以及他们的研究小组表示祝贺，并预祝他们在今后的研究中取得更杰出的研究成果！

可信计算领域值得研究的问题还很多，许多重要的问题和成果等待人们去探索、去获取。目前以云计算、物联网、三网融合为代表的一批新兴信息技术与产业的出现，为可信计算的应用拓展了新的空间。可信计算技术在这里将大有作为。把可信计算技术与它们进行结合，将可产生出更好的成果。

我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决了人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。可信计算是一种确保信息空间安全可信的有效技术。因此，坚持可信计算的研究与开发并让它为确保我国信息安全发挥实际作用，是时代赋予

我们的历史使命。我希望今后能有更多的年轻人投入这一领域的研究！可信计算的明天一定会更辉煌！

中国工程院院士 沈昌祥

致　谢

我们研究小组在可信计算的研究过程中得到国家863计划和国家自然科学基金项目的支持，还得到其他科研项目的支持：

(1)863项目

①可信PDA计算平台关键技术与原型系统研究(2006AA01Z442)

②可信计算平台安全测评关键技术与原型系统研究(2007AA01Z411)

(2)国家自然科学基金项目

①面向军用可信计算环境的构造及评测试验验证研究(91018008)

②多安全等级信息系统的跨域行为安全性研究(61003268)

(3)其他科研项目

我们的研究成果是在这些项目的支持下取得的，因此，我们向所有给予我们项目支持的单位表示衷心感谢！

我们要感谢国家密码管理局！我们在可信计算研究中的许多工作是在国家密码管理局的支持和指导下进行的。

我们要特别感谢瑞达公司！正是在与瑞达公司的合作中我们研制出我国第一款可信平台模块和第一款可信计算平台，以及后续的一些可信计算产品。

最后我们还要感谢一切支持和帮助过我们的领导、专家、同行和用户！

张焕国率全体作者

2010.12.18

前　言

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。信息科学技术得到突飞猛进的发展，取得了辉煌的成就。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。信息和信息技术改变着人类的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备，人们将无法生活和工作。因此，信息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。

当前，一方面是信息科学技术的空前繁荣，可是另一方面危害信息安全的事件不断发生，敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪等，对信息安全构成了严重威胁，信息安全的形势是严峻的。

在信息化社会中，通信、计算机和消费电子的结合，构成了人类生存的信息空间(Cyberspace)。在信息空间中，计算机和网络在军事、政府、金融、工业、商业、等方面的应用越来越广泛，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会的混乱并造成巨大损失。我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决了人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。

因此，信息的获取、存储、传输、处理和安全保障能力成为一个国家综合国力的重要组成部分，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。我国正处在建设有中国特色社会主义现代化强国的关键时期，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可知，信息不能脱离它的载体而孤立存在，因此我们应当从信息系统安全角度来确保信息安全。信息系统的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、网络安全等技术是关键技术。只有从信息系统的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。正是这一技术思想推动了可信计算的产生和发展。

1983年美国国防部制定了世界上第一个《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria，TCSEC)。在TCSEC中第一次提出可信计算机(Trusted Computer)的概念。之后，美国国防部又相继推出了可信网络解释(Trusted Network Interpretation，TNI)和可信数据库解释(Trusted Database Interpretation，TDI)。从

而形成了最早的一套可信计算技术文件。在这套文件中第一次提出可信计算机(Trusted Computer)、可信计算基(Trusted Computing Base, TCB)、可信网络(Trusted Network)和可信数据库(Trusted Database)的概念。多年来这套文件一直成为评价计算机系统安全的主要准则，至今对确保计算机系统安全有重要的指导意义。

1999 年底，IBM、Intel、HP、微软等著名 IT 企业发起成立了可信计算平台联盟(Trusted Computing Platform Alliance, TCPA)，2003 年 TCPA 改组为可信计算组织(Trusted Computing Group, TCG)。TCPA 和 TCG 的出现形成了可信计算的新高潮。欧洲也在 2006 年启动了开放式可信计算(Open Trusted Computing)的研究计划。

可信计算组织 TCG 认为，可信计算的目标是提高计算机系统的安全性。现阶段，可信计算平台应具有确保数据完整性、数据安全存储和平台远程证明等方面的功能。可信计算产品主要用于以下一些领域：安全风险控制，使发生安全事件时的损失降至最小；安全检测与应急响应，及时发现攻击并采取相应措施；电子商务，减少电子交易的风险和损失；数字版权管理，阻止数字产品的非法复制与盗版，等等。

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、到操作系统、再到应用，一级度量认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。

我国在可信计算领域，起步不晚，水平不低，成果可喜。

2000 年 6 月武汉瑞达公司和武汉大学合作，开始研制安全计算机。2003 年研制出我国第一款可信计算平台模块 TPM(J2810 芯片)和第一款可信计算平台，2003 年 7 月 15 日通过国家密码管理局的安全审查。2004 年 10 月通过国家密码管理局主持的技术鉴定。这一新产品被国家科技部等四部委联合认定为“国家级重点新产品”，并得到实际应用。2006 年这一成果获国家密码科技进步二等奖。

2004 年 6 月由瑞达公司和武汉大学联合在武汉大学召开中国首届可信计算平台(TCP)论坛。同年 10 月，在武汉大学召开了“第一届中国可信计算与信息安全学术会议”。

2005 年，联想公司、兆日公司的 TPM 芯片和联想公司的可信计算机也相继研制成功。这些产品也都通过了国家密码管理局的认证。

从 2006 年开始我国进入制定可信计算规范和标准的阶段，在国家密码管理局和国家信息安全标准化委员会的主持下，我国制定了一系列的可信计算规范与标准。我国成为除 TCG 之外唯一拥有自主可信计算规范与标准的国家。

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。

从 2007 年起，我国企业陆续研制出符合我国可信计算规范的可信密码模块芯片和其他可信计算产品。可信计算的实际应用进一步扩大。

至此，我国的可信计算技术与产业取得了辉煌的成绩，我国已经站在国际可信计算领域的前列。

目前以云计算、物联网、三网融合为代表的一批新兴信息技术与产业的出现，为可信计算的应用提供了新的空间。可信计算技术在这里将大有作为。

我们研究小组在可信计算领域开展了一些研究和开发工作，为发展我国可信计算技术与产业作出了一些有益的贡献。

2000 年 6 月我们与瑞达公司合作，开始研制安全计算机。2003 年研制出我国第一款可信计算平台模块 TPM(J2810 芯片)和第一款可信计算平台，并通过国家密码管理局的安全审查。2004 年 10 月通过国家密码管理局主持的技术鉴定。这一新产品被国家科技部等四部委联合认定为“国家级重点新产品”，并得到实际应用。2006 年这一成果获国家密码科技进步二等奖。从 2006 年开始，我们参加了我国一系列的可信计算规范和标准的制定工作。2008 年，在国家 863 计划项目的支持下，我们研制出我国第一款可信 PDA 和可信计算平台测评系统。2009 年我们与瑞达公司合作研制出新的可信平台模块芯片，这款芯片既支持我国的 TCM 规范，又支持 TCG 的 TPM 规范，而且计算资源和密码资源十分丰富。从 2005 年开始，我们与国内外企业合作开展了可信计算应用的研究，取得了令国内外同行高度认可的成果。

通过开展可信计算的研究，我们为国家培养了几十名可信计算方向的博士和硕士研究生，其中许多人已经成为我国可信计算领域的优秀人才。

本书是我们研究小组十年来在可信计算研究方面阶段成果的总结。这些研究成果都是我的博士研究生、硕士研究生得到的。没有他们的创新性研究和勤奋努力，就不可能取得这些研究成果。

全书共分五篇 17 章。第一篇　可信计算概论：第 1 章　信息安全概论，由张焕国撰写。第 2 章　可信计算概论，由张焕国撰写。第 3 章　信任理论，由余发江撰写。第二篇　可信计算平台：第 4 章　可信平台模块，由张焕国和徐明迪撰写。第 5 章　信任链技术，由张焕国和徐明迪撰写。第 6 章　可信软件栈，由严飞和何凡撰写。第 7 章　可信计算平台，由余发江撰写。第 8 章　可信 PC 平台的测试，由严飞，徐明迪和何凡撰写。第 9 章　可信 PDA，由赵波和李晶撰写。第三篇　可信软件技术：第 10 章　软件动态行为可信技术，由彭国军撰写。第 11 章　软件测试技术，由杨飏撰写。第四篇　远程证明与可信网络连接：第 12 章　远程证明，由詹静和张立强撰写。第 13 章　可信网络连接，由张立强撰写。第 14 章　可信网络的授权动态控制，由陈璐撰写。第五篇　可信计算技术应用：第 15 章　基于可信计算技术的数字版权保护，由赵波和李晶撰写。第 16 章　基于可信计算增强网格计算安全，由沈志东撰写。第 17 章　基于可信计算增强云计算基础设施安全，由严飞撰写。全书由张焕国统稿和审校。

武小平博士、涂国庆博士和文松博士为本书提供了初稿，但由于篇幅限制，他们的初稿最后未能写入本书。我向他们表示感谢！

本书的出版只是我们小组在可信计算研究方面阶段成果的总结，并不是可信计算研究的结束，我们小组将会继续深入研究可信计算的理论、技术和应用。我们相信，经过

广大可信计算科技工作者的共同研究，将会取得更加辉煌的研究成果，将会有更多的可信计算优秀论文发表和学术著作出版。

我们小组的可信计算研究得到国家863计划和国家自然科学基金的项目支持，还得到其他科研项目的支持。我们取得的所有研究成果都是在这些科研项目的支持下取得的。没有这些项目的支持，我们的研究是不能顺利进行的。为此，我代表本书的所有作者，向所有给予我们项目支持的单位表示衷心感谢！

我们要感谢国家密码管理局！我们在可信计算研究中的许多工作是在国家密码管理局的支持和指导下进行的。

我们要特别感谢武汉瑞达公司！我们小组的可信计算研究是从与瑞达公司的合作开始的。正是在与瑞达公司的合作中我们研制出我国第一款可信平台模块和第一款可信计算平台，以及后续的一些可信计算产品。

在可信计算的研究过程中，我们得到了我国著名信息安全专家沈昌祥院士、周仲义院士、孙玉院士、任守信研究员、卿斯汉教授、屈延文教授、南湘浩教授、冯登国研究员、何良生研究员、金刚高级工程师等众多专家教授的支持和帮助。没有他们的支持和帮助，就没有我们今天的研究成果。我代表本书的所有作者，向他们表示衷心的感谢！

我代表全体作者衷心感谢给予我们指导、支持和帮助的所有领导、专家和同行！衷心感谢本书的每一位读者！

由于作者学术水平所限，书中难免会有不妥和错误之处。对此，作者恳请读者的理解和批评指正，并于此先致感谢之意。

张焕国

于武汉大学珞珈山

2010年12月18日

目 录

第三篇 可信软件技术

第四篇 远程证明与可信网络连接