普通高等教育“十一五”国家级规划教材

Springer

高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

Trusted Computing Platforms: Design and Applications

可信计算平台：设计与应用

(美) Sean W. Smith 著　冯登国 徐震 张立武 译　蔡吉人 审

http://www.tup.com.cn

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Trusted Computing Platforms: Design and Applications

可信计算平台：设计与应用

(美) Sean W. Smith 著
冯登国 徐震 张立武 译
蔡吉人 审

清华大学出版社
北京

ISBN: 0-387-23916-2

图书在版编目(CIP)数据

可信计算平台：设计与应用/(美)史密斯(Smith, S. W.)著；冯登国，徐震，张立武译. —北京：清华大学出版社，2006.10
(高等院校信息安全专业系列教材)
书名原文：Trusted Computing Platforms: Design and Applications
ISBN 7-302-13174-0

Ⅰ. 可… Ⅱ. ①史… ②冯… ③徐… ④张… Ⅲ. 电子计算机－安全技术－高等学校－教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2006)第 062098 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
责任编辑：张　民
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：14.5　**字数**：300 千字
版　　次：2006 年 10 月第 1 版　2006 年 10 月第1 次印刷
书　　号：ISBN 7-302-13174-0/TP・8331
印　　数：1～3000
定　　价：28.00 元

高等院校信息安全专业系列教材

编审委员会

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已设立了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，国家对信息安全人才的需求量不断增加，但目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整，结构合理，内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足读者对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”现已正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。规划教材将进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着信息安全学科的发展及时修订。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

中国计算机学会教育专业委员会

清华大学出版社

2006年9月

本书序

清华大学出版社给了我一项任务，对冯登国教授等翻译的《可信计算平台：设计与应用》一书进行审校并写一序言，使我有机会先一步领略了该书的全貌。《可信计算平台：设计与应用》是 Sean W. Smith 撰写的一本技术专著，专著系统地阐述了可信计算平台的发展历程，展现了作者 10 年来在探索可信计算方面所做的工作，有以下鲜明特点：

（1）系统性　作者通过介绍可信计算平台研究的先驱者的工作，系统地回答了什么是可信计算平台，可信计算平台是怎样发展来的，如何着手构建可信计算平台，以及拥有了这样的平台能做什么等一系列问题。他提供了可信计算平台从密码加速器、安全协处理器、IBM 4758 到 TCPA/TCG TPM 发展的清晰脉络，将使读者进一步加深对可信计算平台的理解。

（2）实践性　专著的另一个特点是强调理论和应用的密切结合。作者认为，不能只在书本上讨论可能发生的事件，而应尝试在真实世界中付诸应用，消除理论与实践的脱节。作者不仅全面地描述了他领导的工作组所研发的 IBM 4758 安全协处理器的结构，还详细地介绍了对该设备的测试，验证和应用。对 TCPA/TCG TPM（1.1b 版），也通过自己所设计的实验，来验证它的性能和实际应用效果。

（3）前瞻性　作者在分析 IBM 4758 安全协处理器的结构和应用的局限性的基础上，结合 TCPA/TCG TPM 的新成果指出，安全增强硬件构造的专门研究正步入主流计算机平台的发展趋势，并开始进入主处理器和操作系统体系结构融合到一起的发展时期。与此同时，指出可信计算平台的研究焦点将集中在可信计算标准体系结构、可信计算平台的未来设计以及潜在的社会影响等方面。

可信计算已成为当前国际计算机领域的一个研究热点，在我国的研究正

方兴未艾，感谢冯登国教授等的辛苦劳动，以较高的质量翻译了这本技术专著，把它奉献给广大读者。

中国工程院院士

2006 年 8 月

译者序

传统的计算机体系结构因注重标准开放、易用性及效率，对安全性需求考虑甚少，而由体系结构导致的安全性问题越来越突出，为此，国际上高度重视可信计算平台技术的研究，试图研究和开发一种新的计算机安全技术。它从计算机体系结构着手，针对信息系统的安全需求和各种攻击手段，提出一种全新的计算机系统安全解决方案，这将对 IT 技术发展产生重大而深远的影响。目前，这一思想已经成为主流计算平台发展的趋势之一，将对未来信息安全体系产生全面冲击。

我国目前正在积极推进信息安全保障体系建设，这是一项系统工程，涉及技术和管理等多个层面，其中信息安全技术的发展是核心推动力量之一。基于硬件来增强系统和网络的安全性已经在产业界和学术界达成共识，可信计算平台正在融入主流的计算平台。我国企业和研发机构积极从事相关的科研和产品开发工作，已在可信计算平台芯片等方面取得了重大突破。可以预见，可信计算平台的引入即将导致我国信息安全领域的一场变革。

然而，目前我们对可信计算平台的原理和应用模式的理解尚不清晰。本书的出现可谓恰逢其时，它是可信计算领域出版的第一本专著，从理论到实践，给出了领域的技术发展脉络、关键设计技术和应用。本书作者一直工作在可信计算领域的科研和产品开发的第一线，有着雄厚的科研理论功底和丰富的实践经验，这本书就是他的工作成果的总结。

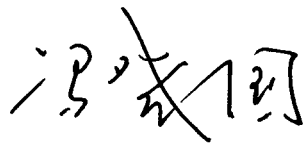
本书从可信计算平台需要解决的问题和相关需求出发，以作者亲自领导的一个可信计算平台实例（IBM 4758 安全协处理器）的研发为主线，对可信计算平台的体系结构、设计和验证等关键技术进行了系统阐述，并介绍了作者基于现有的流行平台 TCG/TCPA TPM 芯片进行的先锋性实验工作和当前可信计算技术发展的一些新方向。本书并不局限于单一平台和相关规范的介绍，而是着眼于整个技术体系，从理论到实践给读者以全面的知识。

虽然可信计算平台是目前的一个研究热点，但有关的系统性的参考资料并不多。信息安全国家重点实验室可信计算平台研究工作组在调研过程中

发现了这本书，并将其作为技术研讨的纲领性材料。随着研讨的深入，我们愈加认识到本书对可信计算平台技术体系把握的深度，也深感翻译本书的必要性。因此，在清华大学出版社的大力支持下完成了本书的翻译工作。相信本书的翻译对国内科研、产业界的研发工作以及标准化工作将起到积极的推动作用。

本书的翻译工作得到了信息安全国家重点实验室可信计算平台研究工作组成员的大力协作。其中，秦宇、陈小峰、于爱民、汪丹、王蕊等博士生和黄亮硕士参与了本书的翻译和审校工作，张妍、李昊、张严、初小博等博士生在技术研讨和翻译过程中做出了一定的贡献。没有他们的鼎力相助，本书的翻译和审校工作不可能进行得如此顺利，在此对他们表示衷心的感谢。

本书的翻译工作得到了清华大学出版社张民编辑的大力帮助，在此表示诚挚的谢意。



2006 年 8 月

原书序

我们正处在一个计算机科学繁荣昌盛的时期。针对安全增强硬件的构造与使用的专门研究已有很长的历史，并且现在逐步将其并入主流计算平台；我们无法预料未来的日子里将发生什么，但肯定会很有趣。本书试图提供一个大致方向。

当前新兴的信息基础设施的一个基本观点是分布式：在分布式环境中，多个参与者参与到计算中，并且其中每一个都可能有不同的兴趣和动机。那么，要检测这种分布式条件下的安全性，就需要检测每个平台做什么计算以及参与者必须信任哪些平台，以此来提供防止各种类型的敌手攻击的安全属性，如果这个参与者想要信任整个计算的话。所以安全分布式计算需要考虑那些参与计算却拥有不同观点的不同组织的独立平台的可信度。我们还必须考虑这么多的参与者实际上是否信任这个平台——并且如果他们应该信任，该如何让他们知道这一点。

硬件是进行计算的基础：此处的硬件是指存储和处理数据位的实际平台（如逻辑门和逻辑电路）。通常我们考虑标准的计算资源——平台为计算问题提供的如内存和 CPU 之类的计算资源。在某些条件下，还通常会考虑平台属性如何对一些难以描述的目标做出贡献，比如对于容错这样的目标的实现。最后，为了更好地解决我们的问题，我们可能会试图改变基础硬件。

将拜占庭分布式问题中可信赖性的重要性和计算平台的硬件基础这两条思路联系起来，我们发现了很多问题。我们期望单个平台具有的合适的可信赖属性是什么？在硬件和高层体系结构中可以采用什么样的方法来达到这些属性？我们能不能在更广的安全应用的计算平台中有效地利用这些可信赖属性？

从当前商业和学术上关于可信计算体系结构的潮流来看，这些是很新的问题。但是从拥有更长历史的安全协处理、安全启动和一些其他经验的角度来看，这些并不是什么新问题。在这本书中，我们将从总体上研究这些问题。我们将深入研究以下领域：一个可信计算平台能提供什么，如何去构建这样

的平台，以及拥有这样一个平台后能做什么。另一方面，我们也将深入研究历史：这些想法是如何在过去那些年，在众多不同的实际平台中提出的，以及这些研究在当前将如何进展。

吸引我研究这一主题的部分原因是因为我曾经在这个领域的发展过程中做了一些工作。工作期间，能够和很多优秀的研究者合作是件非常愉快的事情。本书中的部分内容在我先前的文章[SW99，SPW98，Smi02，Smi01，MSWM03，Smi03，Smi04]中出现过，这些文章会在“进一步阅读”中列出。另外，我的其他一些文章也对相关话题做了深入的讨论。

Sean W. Smith

致谢

本书不只是一本技术专著，同时也展现了我十年来的个人研究探索历程。

我不知道该如何开始感谢所有那些在我的研究中帮助过我的朋友和同事们。我要感谢 Doug Tygar 和 Bennet Yee，当我在 CMU 工作时，是他们给我指出道路，并且从那以后持续不断地给我建议，我们一直保持着很好的关系；我要感谢在 Los Alamos 工作的 Gary Christoph 和 Vance Faber，当我在那里工作时，是他们一直鼓励着我；我要感谢在 IBM Watson 工作的 Elaine Palmer，是他的努力使我们本已死气沉沉的工程变成充满生机的研究和有发展性的成就。我要对 Steve Weingart 和 Vernon Austel 表示特别的感谢，因为他们各自在安全体系和正式建模中与我良好的合作。我还要向 Watson 小组的其余成员表示感谢，包括：Dave Baukus, Ran Canetti, Suresh Chari, Joan Dyer, Bob Gezelter, Juan Gonzalez, Michel Hack, Jeff Kravitz, Mark Lindemann, Joe McArthur, Dennis Nagel, Ron Perez, Pankaj Rohatgi, Dave Safford 和 David Toll；还有在 Vimercate, Charlotte, Poughkeepsie 和 Lexington 的 4758 开发小组的同事们；还要感谢 Mike Matyas。

自从我离开 IBM，很多同事通过富有成效的讨论帮助了我的研究，包括：Denise Anthony, Charles Antonelli, Dmitri Asonov, Dan Boneh, Ryan Cathecart, Dave Challener, Srini Devadas, John Erickson, Ed Feustel, Chris Hawblitzel, Peter Honeyman, Cynthia Irvine, Nao Itoi, Ruby Lee, Neal McBurnett, Dave Nicol, Adrian Perrig, Dawn Song 和 Leendert van Doorn。在学术界做研究，需要购买仪器、机票，还要付给学生们薪水；这些工作的资金部分来自于 Mellon 基金、美国国家自然科学基金会（NSF）（CCR-0209144 项目）、AT&T/Internet2 和国土安全部国内应急办公室（2000-DT-CX-K001 项目）的支持。

在 Dartmouth，我的学生们也加入了我的研究之旅，他们包括：Alex Barsamian, Mike Engle, Meredith Frost, Alex Iliev, Shan Jiang, Evan

Knop，Rich MacDonald，John Marchesini，Kazuhiro Minami，Mindy Periera，Eric Smith，Josh Stabiner，Omen Wild 和 Ling Yan。那些在 Dartmouth PKI 实验室和计算机科学系的同事们也提供了对研究有极大帮助的讨论，当然也少不了咖啡。

Dartmouth 的学生 Meredith Frost，Alex Iliev，John Marchesini 和 Scout Sinclair 甚至提供了更多的帮助，他们通读并修订了手稿的早期版本。

最后，我要感谢我的家人长久以来对我的支持和理解。

Sean W. Smith
Hanover，New Hampshire

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602　　计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：可信计算平台：设计与应用

ISBN：7-302-13174-0/TP・8331

个人资料

姓名：_____ 年龄：_____ 所在院校/专业：_____

文化程度：_____ 通信地址：_____

联系电话：_____ 电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

_____

_____

您希望本书在哪些方面进行改进？（可附页）

_____

_____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。

目 录