HZ BOOKS
华章教育

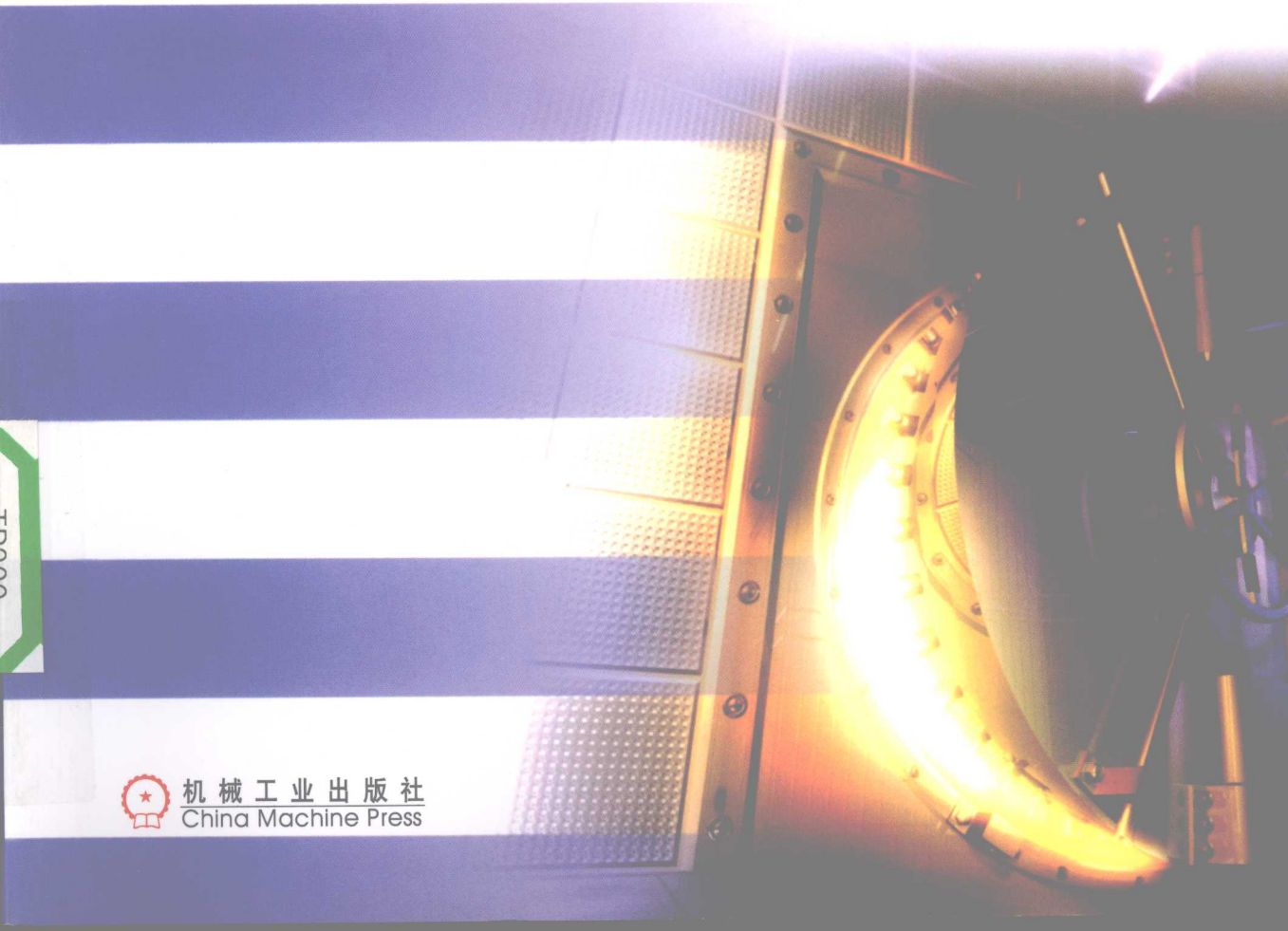
IBM
PRESS

可信计算

A Practical Guide to Trusted Computing

(美) David Challener　Kent Yoder　Ryan Catherman
David Safford　Leendert Van Doorn　著

赵 波　严 飞　余发江　等译
张焕国　审校



机械工业出版社
China Machine Press

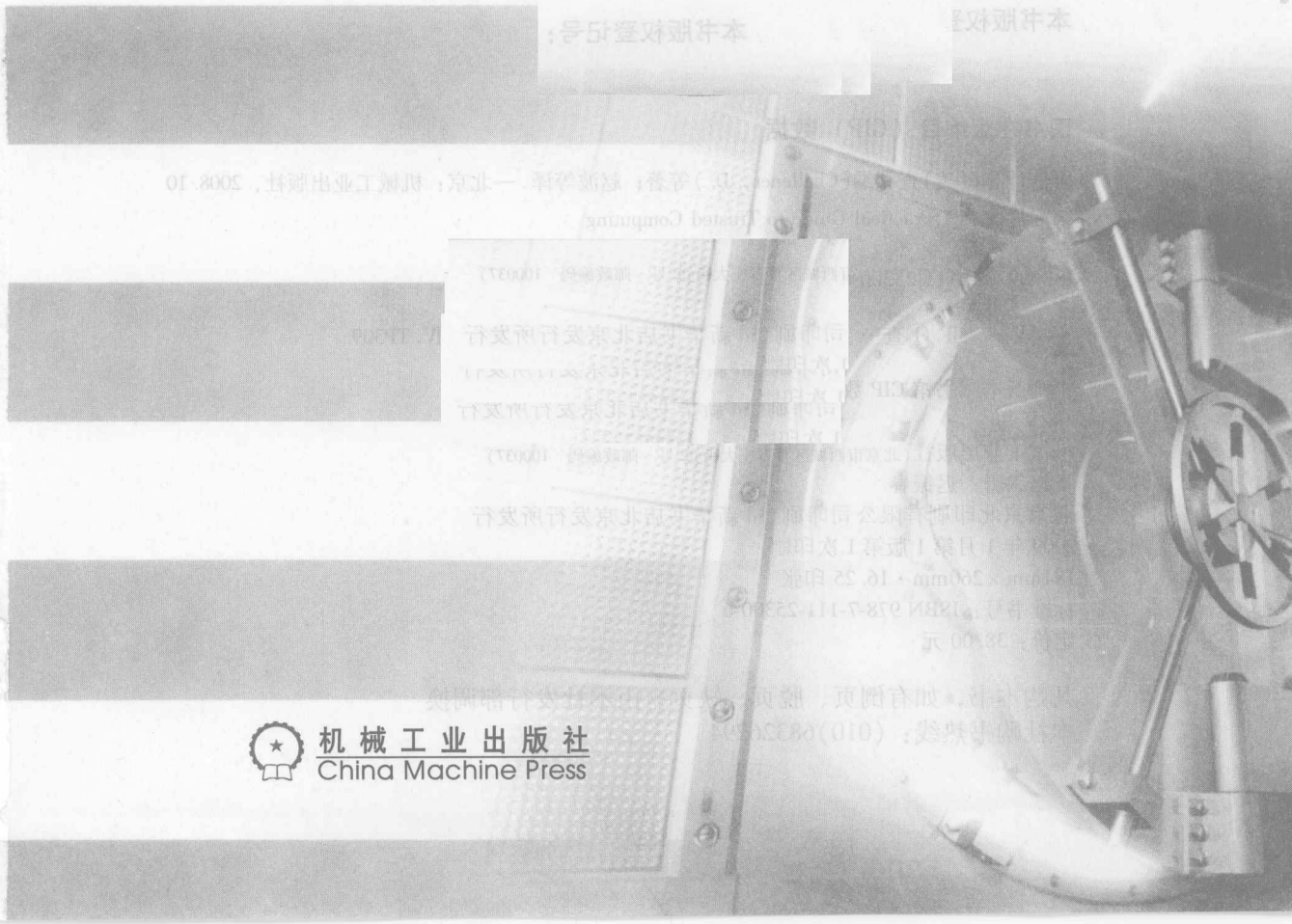
可信计算

A Practical Guide to Trusted Computing

(美) David Challener　Kent Yoder　Ryan Catherman
David Safford　Leendert Van Doorn　著

赵 波　严 飞　余发江　等译

张焕国　审校



机械工业出版社
China Machine Press

本书围绕不断快速发展的可信计算学科展开全书内容，其内容涵盖了如何使用可信计算模块（TPM）提供安全解决方案，并讨论了如何编码实现。本书介绍了 TPM 的基本功能以及如何编写代码通过标准 TCG（Trusted Computing Group，可信计算组织）软件栈访问这些功能，同时还提供了相关范例，并讨论了利用 TPM 能够实现的解决方案。

本书简明实用，可作为高等院校相关专业的教材或教学参考书，同时也适合软件工程师、软件项目经理和技术主管、用户界面设计者和可信计算爱好者阅读。

本书版权登记号：图字：01-2008-3692

图书在版编目（CIP）数据

可信计算/（美）查利纳（Challener，D.）等著；赵波等译. —北京：机械工业出版社，2008.10
书名原文：A Practical Guide to Trusted Computing

ISBN 978-7-111-25300-6

Ⅰ. 可…　Ⅱ. ①查…　②赵…　Ⅲ. 电子计算机－安全技术　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2008）第 154544 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：迟振春
北京京北印刷有限公司印刷 · 新华书店北京发行所发行
2009 年 1 月第 1 版第 1 次印刷
184mm × 260mm · 16.25 印张
标准书号：ISBN 978-7-111-25300-6
定价：38.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

译 者 序

随着计算机和网络技术的迅速发展与广泛应用，社会的信息化程度提高，使用计算机和网络进行信息存储、通信和处理成为人们生活和工作中不可缺少的组成部分。如果计算机和网络的信息安全受到危害，将会危及国家安全，引起社会混乱，造成重大损失。因此，确保计算机和网络的信息安全成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。

通过信息安全的实践，人们逐渐认识到，大部分对信息系统的攻击来自终端，因此应当采取措施提高终端的安全性，从源头上阻止对信息系统的攻击。

众所周知，信息系统的硬件结构安全和操作系统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。而且，必须从底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。对于最常用的微机终端，必须从芯片、主板、BIOS、操作系统、网络等方面综合采取措施，才能确保微机系统的安全。正是这一技术思想，催生了可信计算。

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)和可信计算基(Trusted Computing Base，TCB)的概念。1984 年，又制定了《可信数据库解释》(Trusted Dadabase Interpretation，TDI)和《可信网络解释》(Trusted Network Interpretation，TNI)。于是，形成了“彩虹”系列技术文件，它标志着可信计算的初现。此后，“彩虹”系列技术文件一直成为评价计算机系统安全的主要准则，至今仍对计算机系统安全有指导意义。但是随着信息技术的发展，“彩虹”系列技术文件呈现出一定的局限性，包括：主要考虑信息的秘密性，而对完整性、真实性考虑较少；强调系统安全性的评价，并没有给出达到这种安全性的系统结构和主要技术路线。

1999 年，IBM、HP、Intel、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)。TCPA 的成立，标志着可信计算高潮阶段的出现。2003 年，TCPA 改组为可信计算组织(Trusted Computing Group，TCG)，标志着可信计算技术和应用领域的进一步扩大。TCPA 和 TCG 的出现形成了可信计算的新高潮。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。2006 年，欧洲启动了名为“开放式可信计算”(Open Trusted Computing，OTC)的可信计算研究计划。目前，国外企业已经推出了一系列的可信计算产品。与“彩虹”系列技术文件相比，TCG 可信计算具有如下重要意义：提出可信计算机平台的概念，并具体化到微机、PDA、服务器和手机平台，且给出了体系结构和技术路线。它不仅考虑信息的秘密性，更强调了信息的真实性和完整性，从而使其更加产业化和更具广泛性。

我国在可信计算领域起步不晚，各级政府都大力支持可信计算的研究与产业化发展。各企业已经推出了一些可信计算产品和应用系统，政府主持制定了一系列的可信计算技术规范，高等院校和科研院所也在可信计算理论和关键技术方面取得了丰硕的成果。2007 年，我国成立了“中国可信计算联盟”。我国可信计算技术与产业的发展已经站在国际可信计算领域的前列。

实践已经证明，可信计算是增强信息系统安全的一种行之有效的新技术。正是由于可信计

算是一种新技术，所以目前关于可信计算的书籍很少。广大科技工作者和研究生迫切需要一本实用的可信计算书籍，为此，机械工业出版社引进出版了这本《可信计算》。

《可信计算》是第一本对可信计算本质进行深入探讨的专著，是一本难得的好书。其内容涵盖了如何使用可信计算模块(TPM)提供安全解决方案，并讨论了如何编码实现。书中既介绍了可信计算的基本技术思想，又介绍了TPM的基本功能以及如何编写代码通过TCG软件栈(TSS)调用这些功能，同时还提供了相关范例，并讨论了利用TPM解决实际问题的技术方案。

本书的五位作者都是可信计算领域的著名专家，他们参与了TCG软件栈(TSS)规范的制定，其中第一作者David Challener担任TCG TSS委员会的主席。他们都直接编写过使用TPM的软件，还开办了可信计算研讨班讲授相关课程。他们具有丰富的TPM和TSS方面的实践经验。

本书的最大特点是简明实用，既可以作为信息领域科技人员的技术参考书，也可以作为高等院校相关专业的教材或教学参考书。

本书由赵波、严飞、余发江等翻译，张焕国审校。詹静、徐明迪、何凡、张立强、陈璐、文松、杨飏、徐士伟、童言、邹冰玉、李晶、黄祥梨、王莉、向骕、韩碧霞、汤梅、张雨、李小菲也参与了部分翻译工作和书稿整理工作。

由于译者的专业知识和外语水平有限，书中错误在所难免，敬请广大读者批评指正，在此先致感谢之意。

译者

2008年9月18日

前　言

目前，可信平台模块(Trusted Platform Module，TPM)成为世界各大PC供应商积极推广的一类新产品。本书作为第一本关于正确使用TPM的工具书，向用户展示可信计算技术的风采，并指导用户进行相关的开发工作。

本书内容

本书围绕快速发展的可信计算学科展开内容。近几年来，随着病毒、木马以及间谍软件数量的快速增长，安全问题呈现出愈演愈烈的状态，用户急需一种新的方法为他们提供更为安全的保障。目前，尽管已经有一些书对可信计算理念进行了讲述，但本书是第一本对可信计算本质进行深入探讨的专著，其内容涵盖了如何使用TPM提供安全解决方案，并讨论了如何编码实现。本书介绍了TPM的基本功能以及如何编写代码通过标准TCG(Trusted Computing Group，可信计算组织)软件栈访问这些功能，同时还提供了相关范例，并讨论了利用TPM能够实现的解决方案。

在本书的撰写过程中，几位作者正从事将TSS 1.1规范扩展到TSS 1.2规范的工作。TSS 1.2可以访问由TPM 1.2提供的新功能，本书在第14章中介绍了TPM 1.2的新功能，所以对于那些试图将TSS代码放在任意TPM上工作的读者，可以跳过这一章；而对于那些想使用TPM 1.2新功能的读者，可以将第14章纳入学习过程中。

本书的作者都是可信计算领域的专家，他们参与了TSS栈相关规范的编写，并直接编写过使用TPM的软件。此外，他们还开办了研讨班讲授相关课程，同时发表了如何使用TPM的论文。

相关基础知识

本书的代码都是基于C语言的，所以C语言代码的阅读能力是理解范例的必要条件。此外，读者应具有一定的密码学基础——特别是对称公钥密码、非对称公钥密码以及散列密码。本书简单介绍了这些概念，但没有对算法进行详细描述。对于想深入研究此内容的读者，Bruce Schneier的《应用密码学》[⊖]是一本不错的参考书。如果只是想体会一下TCG的优点，本书的第一部分和第三部分值得推荐。如果读者在思考一个特定项目，本书的所有篇章都会对你有所帮助。

读者群体

本书提供了编写、使用TPM软件的具体细节。如果读者不熟悉可信计算并想编写利用TPM功能的代码，那么整本书都是有价值的。如果想了解TPM的设计及其本质，就需要重点研究第一部分和第二部分。

⊖ 本书中文版已由机械工业出版社引进出版。——编辑注

适用于软件工程师

本书介绍了所有与 TPM 编程相关的内容，提供了一些已经编译通过的范例，实现了真实的功能要求。此外，为帮助读者理解这些代码的真实含义，本书还解释了这些代码的设计理论，同时提供了代码注释。

如果想了解待解决问题的复杂性，请阅读第 1 章。如果想了解 TPM 的功能，请阅读第 2 章以及第 3 章。如果想了解使用 TPM 的功能可以解决何种问题，请阅读第 11 到 13 章。如果已经理解 TPM 的功能并想使用 TPM 1.1 编写程序，请阅读第 4 到 10 章。如果想使用 TPM 1.2 的扩展功能，请阅读第 14 章。

适用于软件项目经理和技术主管

软件项目经理需要理解 TPM 的功能与项目体系结构之间的关系。在任何安全程序中，最重要的是在编码之前建立完善的体系结构。体系结构设计上的缺陷将导致大量安全漏洞的出现。

本书将帮助读者设计和理解基于 TPM 功能的安全系统体系结构的关键问题。尤其是第 1、2、3、11、12、13 和 14 章，对于项目经理将非常有用。

适用于用户界面设计者

易用性和安全之间一直是一对不可调和的矛盾需求，而本书的第 11、12 和 13 章则为用户界面设计者提供了改进安全方案易用性所需的信息。

适用于可信计算爱好者

如果读者考虑使用 TPM，请参阅第 1 ~ 3 章和 11 ~ 13 章，这些章节叙述了可信计算能解决的问题及其在体系结构方面的解决方法。

适用于 TPM 的熟练用户

对于具有 TPM 使用经验的用户，如果对使用 TPM 还能实现什么功能感兴趣的话，本书（特别是书中第 11、12、13 和 14 章）可能会给您带来灵感。毕竟他山之石可以攻玉！

本书的结构

第一部分：背景材料

第一部分是可信计算概述，包括可信计算产生的背景、所解决的问题及可信平台模块提供的功能。

第 1 章　可信计算概述

目前，黑客的注意力已经逐渐从网络和服务器转移到客户端。本章介绍当前面向客户端的安全攻击概况及其严重性，并解释 TPM 对于解决该问题的优势。本章也讨论隐私问题，并向程序员给出避免产生该问题的建议。

第 2 章　可信平台模块的设计目标

最初设计 TPM 规范时，专家们就提出了设计需求及目标。本章通过讨论这些设计目标使读

者从广义上对 TPM 有所了解，并建立必要的背景知识，从而理解 TPM 实现的具体特性。

第 3 章　可信平台模块功能概述

本章从体系结构的角度考察规范设计，对 TPM 1.1 所能实现的具体特性及其实现方式进行描述。通过阅读本章，读者将会对 TPM 所能解决的问题有所认识。此外，还讨论了规范中某些被忽略的特性。

第二部分：TCG 编程接口

第二部分的内容适合于程序员学习。通过学习范例，对软件栈接口进行深入研究。首先，从底层设备驱动程序的通信开始，到计算机系统的启动过程以及如何使用 TPM 进行安全加固，然后讨论软件栈提供的核心服务，以及远程应用程序使用 TPM 时的接口通信问题。以此为主线，后面几章讨论在高层上使用 TPM 的应用接口。

第 4 章　编写 TPM 设备驱动程序

本章提供用于编写与 TPM 通信的设备驱动程序的必要信息，这对于希望在现有操作系统（Windows、Linux）之外使用 TPM 的读者来说尤为重要。

第 5 章　底层软件：直接使用 BIOS 和 TDDL

本章提供不通过 TSS 栈与芯片直接通信的方法，这对于编写在 BIOS 中运行的代码或在新操作系统或内存受限环境中编写 TSS 栈都很重要。本章最初实现于 Linux 平台，不过已经修改为系统无关模式。此外，本章向使用 TSS 栈的用户提供真实的体会，以便他们了解底层完成的具体工作。

第 6 章　可信启动

本章描述如何使用 TPM 芯片来度量平台的安全状态。目前，有两种实现方式：1.1 版本中的静态可信根和 1.2 版本中的动态可信根。书中对这两者都有详细描述，而且所用范例代码也展示了如何实现状态度量。这是本书中少有的经过测试的 1.2 版本的代码之一，因为这些接口并不需要目前还不存在的 1.2 版本 TSS 栈。

第 7 章　TCG 软件栈

TSS API 是访问 TPM 的最通用接口。本章描述 TSS 体系结构、使用 API 的约定以及软件对象类型的使用。通过一些简单 TSS API 示例程序，可以区分 1.1 API 和 1.2 API 编程的不同之处。

第 8 章　使用 TPM 密钥

密钥管理在安全程序中是最难实现的功能之一，而这正是 TPM 的优点之一。本章详细描述密钥的创建、存储、装载、迁移与使用并给出范例。对特定的密钥（如认证密钥、存储密钥和签名密钥），配合使用的示例给予说明。

第 9 章　使用对称密钥

本章介绍如何在应用中使用 TPM 提供的对称密钥。对于有兴趣使用 TPM 进行整体加密，从而加强应用程序安全性的读者来说，阅读本章可以学会如何利用 TPM 的特性来加强安全。

第 10 章　TSS 核心服务（TCS）

核心服务层在正常应用程序接口 API 的下层。对于应用程序开发者而言，了解这些服务提供的内容可以帮助他们准确理解每个 API 的功能。此外，如果应用程序开发者想开发一个客户/服务器程序，TPM 需要提供远程服务，那么核心服务层就是被调用的应用层。本章深入分析核心服务机制并提供执行远程调用的范例代码。

第 11 章　公钥加密标准 PKCS#11

本章给出了使用 TSS 的真实范例程序，提供一个将 PKCS#11 栈与 TSS 栈相联系的完整工程实例。该实例可以向应用程序提供中间件服务，其中的代码有注释并可以开源使用。

第三部分：体系结构

第三部分主要介绍可信计算软件栈的功能，以及规范撰写者在设计体系结构时的设计理念。即使读者对编写特定的应用程序不感兴趣，阅读这些章节也会有助于解释设计时所做的决策。

第 12 章　可信计算和安全存储

TPM 通过两个命令提供安全存储功能：BIND 和 SEAL。本章提供一些范例，解释如何使用这些命令向终端用户提供功能，同时也讨论了安全实现时应该解决的某些问题。阅读本章有助于读者理解这两个命令的设计思想。

第 13 章　可信计算和安全认证

TPM 提供芯片内部的安全签名功能。本章给出一些使用命令的范例，这些范例可用于一些实际的应用以帮助用户解决实际问题。阅读本章将有助于读者理解签名命令的设计准则。

第 14 章　可信设备管理

大规模部署 TPM 时，如何有效管理这些 TPM 将尤为重要。本章关注如何使用迁移命令来提供 TPM 的远程管理。

第 15 章　辅助硬件

TPM 的设计定位是一种廉价的硬件设备，因此不能仅仅依靠 TPM 解决所有的安全问题。但是，它可以向其他的安全设备提供大量可利用的功能。本章介绍一些增强客户端安全的方法。

第 16 章　从 TSS 1.1 到 TSS 1.2

TSS 1.2 规范已于最近发布。这一章介绍新规范中提到的新功能，并给出每个功能如何使用的范例代码。新功能包括：CMK、代理、DAA、新的 PCR 行为、Locality、NVRAM、审计、单调计数、传输、时钟中断和管理命令。本章适合试图使用新功能来编写代码的读者，代码只能在使用 TPM 1.2 的客户端上运行。

第四部分：附录

第四部分可以帮助读者快速查找 API 的特定功能。对于直接与硬件或可信计算软件栈通信的函数，附录中还分别提供了 TPM 命令参考和 TSS 命令参考。这些参考对命令均做了简短描述，并都给出了使用方法。

附录 A　TPM 命令参考

该附录包括 TPM 级的命令、命令使用的环境及其功能的简要描述。

附录 B　TSS 命令参考

该附录包括 TSS 级的命令、命令使用的环境及其功能的简要描述。

附录 C　函数库

该附录包括帮助函数和函数的描述信息，这些函数可以帮助用户创建使用 TPM 的程序。

附录 D　依据对象和 API 级别划分 TSS 函数

该附录根据受内部 TSS 对象影响与 API 交互的级别来对函数进行分类。在编写代码时，该分类信息可以用于快速查表以确认 API 函数是否可用。

一些本书的评阅者指出，从 TPM 应用的角度思考将有助于理解 TPM 设计的依据。作者希望本书能够帮助读者理解 TPM，而且可以推进 TPM 资源的有效利用。

致谢

特别感谢本书的评阅者提出许多宝贵的修改意见，他们是：David Grawrock、Ken Goldman、Sean Smith 和 Emily Ratliff 等。

关于作者

David Challener　美国伊利诺伊大学厄巴纳－尚佩恩分校应用数学专业博士。在纽约州 East Fishkill 加入 IBM 公司之后，设计了第一个 TPM(代表 IBM 公司)，其后成为 TCG TSS 委员会的主席。在 IBM PC 拆分出售给 Lenovo 后，加入 Lenovo 公司。此后，作为 Lenovo 公司的代表加入 TCG 技术委员会、TPM 工作组以及许多其他组织，并担任 TSS 委员会主席。目前，他是 Lenovo TCG 委员会成员。

Kent Yoder　2001 年在美国普度大学获得计算机科学学位后，一直在 IBM Linux 技术中心工作。作为 IBM 的代表加入 TCG TSS 委员会，编写和维护 TrouSerS(在 TCG TPM 硬件上执行的符合 TSS 软件规范的开源 TSS 库)。

Ryan Catherman　在 IBM 工作期间是可信计算组的成员，拥有 TSS 和 TPM 工作组会员资格。他是 IBM 可信计算软件初始时期的合著者之一，以及该软件 UNIX 版本的创始人。现在，他在 Opsware 公司工作(该公司最近被惠普收购)，并获得计算机工程硕士学位。

David Safford　位于美国纽约州 Hawthorne 的 IBM T. J. Watson 研究中心研究人员。他在许多领域进行安全研究，包括道德黑客(ethical hacking)、威胁分析、安全工程、入侵检测传感器、漏洞扫描、密码学和操作系统安全。在 1996 年加入 IBM 公司之前，他是得克萨斯大学 A&M 分校超级计算和网络研究所的主任，还是美国海军 A-7 飞行员。

Leendert Van Doorn　AMD 的高级研究员，负责软件技术办公室的工作。他在荷兰阿姆斯特丹自由大学获得博士学位，从事微内核设计与开发。现在，他的研究方向包括运行系统管理、加速计算(即 AMD 的异构和同构的多核计算)、安全和虚拟技术。在加入 AMD 之前，他是 IBM 公司 T. J. Watson 研究中心的高级经理，负责管理安全系统和安全分析部门，之前曾从事 FIPS 140-2 四级物理安全协处理器、可信系统和虚拟化研究，是可信计算组委员会成员。在 IBM 的虚拟化战略中，他创建并领导 IBM 的安全虚拟化监视器(hypervisor)和可信虚拟数据中心的研究工作。此外，他开发了 Xen 的开源安全虚拟化监视器，例如，整合对 AMD-V 和 Intel VT-x 的支持代码。

目　录

第一部分

背景材料

第1章　可信计算概述

本书主要描述由可信计算组织（Trusted Computing Group，TCG）定义的可信平台模块（Trusted Platform Module，TPM），它是一种置于计算机中的新的嵌入式安全子系统，同时还将介绍 TPM 的相关知识和实际应用方法。本书并没有限于对 TPM 功能和应用编程接口（API）标准的描述，而是通过很多实例，告诉读者 TPM 到底能够解决什么问题，以及规范中所做设计决策的理由。读完这本书，读者应该更好地了解目前存在于 PC 客户端的安全问题，以及如何利用 TPM 的功能去解决这些问题。下面来看看 TPM 能够为客户端的安全做些什么。

在本章中，有三个问题需要注意：

- 目前安全威胁问题非常严峻。
- 不能仅仅靠软件来抵抗安全威胁。
- TPM 是专门用来抵抗安全威胁的。

同时，本章还要简要地讨论 TPM 在保护隐私方面所起的作用。

1.1　计算机安全攻击所造成的损失是惊人的

虽然目前不能确切地知道电脑犯罪造成的经济损失，但可以基于某些已知的数据和调查来进行估计。统计结果显示电脑犯罪是非常令人担忧的：

- “电脑犯罪在 2004 年造成了 1050 亿的损失，远远高于非法药品销售所造成的损失。”——Valerie McNiven[1]。
- “身份欺诈所造成的损失在 2004 年到达了 526 亿。”——Javelin 决策和研究机构[2]。
- “美国一年花费了 672 亿美元对付病毒、间谍软件、PC 盗窃以及其他与电脑相关的犯罪。”——FBI[3]。
- 超过 130 次的电脑入侵将至少 5500 万美国人的个人数据偷走，如社会保险号和信用卡号。——《今日美国》[4]。

而这些仅仅是冰山一角。作者经常与一些人和公司交流，他们的电子银行都遭遇过黑客的非法入侵，导致账户被洗劫一空。还有很多人都经历过这样的事情——由于系统被病毒或间谍软件感染而不得不花几小时重装 PC 的操作系统。许多人由于受到计算机欺诈（如“网络钓鱼”）而导致身份信息被盗，同时暴露了大量个人信息（如社会保险号）。近来，以客户 PC 为主的安全威胁越来越多。下面继续看看这些安全威胁的问题和趋势。

1.2　正在变化中的计算机安全威胁

黑客攻击客户端是目前计算机安全普遍的趋势。在 20 世纪 80 年代，黑客通过破译口令和拦截网络会话来攻击网络。当应用程序对通过网络的数据加密时，黑客开始利用错误配置的服务和有 bug 的服务漏洞来攻击服务器，例如 Web 服务器。公司采用防火墙入侵检测机制和安全审计工具应对这些攻击，以保护服务器。因此，黑客开始把攻击方向转向无保护的客户端。