HZ BOOKS
华章科技

Apress®

· 网络空间安全技术丛书 ·

A PRACTICAL GUIDE TO TPM 2.0

Using the Trusted Platform Module in the New Age of Security

TPM 2.0 原理及应用指南

新安全时代的可信平台模块

[美] 威尔·亚瑟（Will Arthur）大卫·查林纳（David Challener）著
王鹃 余发江 严飞 张立强 石源 等译
张焕国 李彦 赵波 等审校

- 技术规范通常是难于理解的用户手册，TPM 2.0 规范也不例外。
- 本书旨在对 TPM 2.0 规范进行深度解读，让开发人员更好地理解该规范，尤其是那些需要了解底层细节的开发人员。

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

TPM 2.0 原理及应用指南

新安全时代的可信平台模块

A PRACTICAL GUIDE TO TPM 2.0

Using the Trusted Platform Module in the New Age of Security

[美] 威尔·亚瑟（Will Arthur）大卫·查林纳（David Challener）著
王鹃 余发江 严飞 张立强 石源 等译
张焕国 李彦 赵波 等审校

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

TPM 2.0 原理及应用指南——新安全时代的可信平台模块 /（美）威尔·亚瑟（Will Arthur），（美）大卫·查林纳（David Challener）著；王鹃等译 . —北京：机械工业出版社，2017.9
（网络空间安全技术丛书）
书名原文：A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security

ISBN 978-7-111-58201-4

I. T… II. ① 威… ② 大… ③ 王… III. 全面设备管理－研究 IV. F273.4

中国版本图书馆 CIP 数据核字（2017）第 241943 号

本书版权登记号：图字 01-2017-2053

TPM 2.0 原理及应用指南——新安全时代的可信平台模块

出版发行：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：张梦玲　　责任校对：李秋荣
印　　刷：北京文昌阁彩色印刷有限责任公司　　版　　次：2017 年 10 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：18.75
书　　号：ISBN 978-7-111-58201-4　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

华章科技
HZBOOKS | Science & Technology

Foreword 序

随着信息技术与产业的高速发展和广泛应用，人类社会进入了信息化时代。在信息化时代，一方面信息技术和产业高速发展，呈现出空前繁荣的景象；另一方面危害信息安全的事件不断发生，形势十分严峻。信息安全事关国家安全、事关社会稳定。因此，必须采取措施确保我国的信息安全。

当前，云计算、大数据等新技术突飞猛进地发展，并逐步广泛运用。这些新技术的发展和应用给人们带来极大的便利，但同时也给信息安全提出了一些新的挑战。

云计算是面向服务的计算：基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。云计算旨在使计算像水、电、油一样，成为公共基础资源，因此可以极大地降低用户的开支。但是，面向服务的计算在工作模式上必然是资源共享，而资源的共享将引发诸多信息安全问题。例如，基础设施和平台安全问题：云计算有几乎无限的计算资源（基础设施、平台和软件），但是用户不知道这些资源是否可信。服务安全问题：云计算有几乎无处不在的服务，但是用户不知道这些服务是否可信。数据安全问题：云计算有几乎无限的存储空间，但是用户不能感知自己数据的存在、不知道自己的数据存储在哪里，更不能控制自己的数据。于是，用户就不信任云计算，不信任自然就不会应用。

大数据处理与云计算是一对“双胞胎”。一方面，云计算有几乎无限的存储能力；另一方面，大数据需要巨大的存储空间。因此，大数据必然存储在云计算的存储系统中。同时云计算有几乎无限的计算能力；而大数据处理需要巨大的计算能力。因此，大数据必然由云计算系统进行处理。只有这样结合，才是最合理、最节省的方案。由此可见，云计算与大数据的开发应用与安全可信是彼此联系在一起的。于是，云计算的安全问题也会影响大数据的安全。反过来，大数据带来的隐私保护和密码的工作效率等问题，也会影响云计算安全。

可信计算是一种旨在增强计算机系统可信性的综合性信息安全技术，特别适用于提高信息系统的基础设施和平台的可信性。很多年前，张焕国教授就提出“可信≈可靠＋安全”的通俗观点。这也就是说，稳定可靠和安全保密是可信性的主要方面。因此，采用可信计算技术增强云计算、大数据系统的可信性，已成为一种必然的选择。

中国在可信计算领域起步很早、成果可喜、有很多创新，整体水平处于国际前列。早在2003年，武汉瑞达公司就和武汉大学合作开发出中国第一款嵌入式安全模块和第一款可信计算机（SQY14嵌入密码型计算机），并得到实际应用。

英特尔（Intel）公司是国际可信计算组织（TCG）的发起单位之一，为可信计算做出了重要贡献。为了介绍可信计算技术的新进展和可信计算在云计算基础设施中的安全作用，在英特尔的组织下，ApressOpen出版了3本可信计算和云系统安全的技术图书，现由机械工业出版社华章公司引进，中文版会在2017年9月至2017年10月陆续出版。

①《A Practical Guide to TPM 2.0：Using the Trusted Platform Module in the New Age of Security》（中文版：《TPM 2.0原理及应用指南——新安全时代的可信平台模块》）。TPM 2.0是TCG标准，也是国际标准，并得到中国国家密码管理局的支持。TPM 2.0扩展了加密算法灵活性，支持中国商用密码算法。

②《Intel Trusted Execution Technology for Server Platforms：A Guide to More Secure Datacenters》（中文版：《面向服务器平台的英特尔可信执行技术——更安全的数据中心指南》）。英特尔用TXT技术把以上TPM标准和物理机的可信扩展到虚拟环境（VMM）和虚拟机（VM），并结合Intel VT虚拟技术把虚拟机的隔离、可信和安全做得更好。

③《Building the Infrastructure for Cloud Security, A Solutions View》（中文版：《云安全基础设施构建——从解决方案的视角看云安全》）。在以上TPM标准和TXT技术基础上，通过远程认证（OAT）和云完整性技术（CIT）把可信扩展到完整云安全基础设施和所有数据中心安全。

这些可信基础设施包括可信软件定义的存储（Trusted SDS）、可信软件定义的网络（Trusted SDN）、可信交换机（Trusted Switch），直至可信软件定义数据中心和基础设施（Trusted SDDC或Trusted SDI）。

这些数据中心安全技术可扩展到：大数据安全和隐私保护、端到端物联网的安全、5G网络安全、智慧城市安全、精准医疗安全和隐私保护等。

所以说，以上三本书是技术上非常相关、由下而上渐进、自然延伸扩展的可信云计算安全图书。

2012年6月，武汉大学和英特尔发起、与多家企业联合成立了中国可信云社区（ChinaSigTC）。宗旨是，基于中国商用密码和可信计算标准，发展中国可信云计算技术与产业。工作方式是，通过开放开源和自主开发，一起研发中国本土化可信云安全解决方案。为全面支持开源和本土开发，英特尔开源了UEFI BIOS及其TPM 2.0安全模块、TPM 2-TSS可信软件栈、Tboot TXT可信启动模块、OAT开源远程认证技术和OpenCIT云完整性技术。这些都与这三本书中的内容密切相关。中国可信云社区也开源了GMSSL国密OpenSSL等。该社区的活动推动了可信云计算的本土化发展。（相关内容请参考本书附录。）

这三本书也是该社区技术工作的重要参考书。2012~2014年，该社区的国民技术、中标软、武汉大学与英特尔合作一起开发了支持中国商用密码的TPM2.0芯片、BIOS及其OS

驱动。2014~2015 年，该社区的华为、浪潮、大唐公司分别与英特尔和武汉大学合作开发出自己的可信云服务器，全面支持 TPM 2.0/TXT 、可信虚拟化、远程认证和安全可信管控，并实现了产业化。这些产品的开发和应用，从实践上证明了采用可信计算增强云计算、大数据系统安全是十分有效的。2016 年至今，该社区的大唐、英特尔、XSKY、XNET 和武汉大学一起合作开发出可信存储、可信交换机、可信软件定义的数据中心（Trusted SDDC/SDI），从实践证明可信计算技术完全可以扩展到整个数据中心的所有计算、存储、网络节点并得以统一的 CIT 认证，从而大大提高整个系统的可信性。

全面实现信息系统安全可信，任重而道远，让我们和社区一起

将可信进行到底！

为满足社区成员的需要，也为了使广大中文读者能够读到这三本书，在英特尔公司的支持下，机械工业出版社华章公司组织武汉大学和北京工业大学的老师把它们翻译成中文并出版发行。其中《 TPM 2.0 原理及应用指南——新安全时代的可信平台模块》由武汉大学的老师翻译，《云安全基础设施构建——从解决方案的视角看云安全》和《面向服务器平台的英特尔可信执行技术——更安全的数据中心指南》由北京工业大学的老师翻译。

这三本书内容丰富、新颖实用，是难得的好书。本书可作为从事信息安全、计算机、通信、电子信息等领域的科技人员的技术参考书，也可用作信息类专业的教师、研究生和高年级本科生的教学参考书。

相信这三本译著的出版发行将会促进可信计算、云计算安全、大数据处理系统安全等领域的技术交流、进步和产业发展。

由于译者的专业知识和外语水平有限，我们也请了中国可信云社区和英特尔中国技术的专家一起校阅，但书中错误在所难免，敬请读者指正，我们在此先致感谢之意。

张焕国（于武汉大学珞珈山）

李彦（于英特尔上海紫竹）

2017 年 8 月

译 者 序 The Translator's Words

可信计算是增强信息系统安全的一种行之有效的技术。它基于一个硬件安全模块，建立可信的计算环境。可信硬件安全模块担任信任根的角色，通过密钥技术、硬件访问控制技术和存储加密等技术保证系统和数据的信任状态。基于可信硬件安全模块，可建立从硬件可信根→ BIOS →操作系统→应用系统的信任链，从而检测和验证系统的可信性。

可信平台模块（Trusted Platform Module，TPM）是可信计算中一种植于计算机内部为计算机提供可信根的芯片。该芯片的规范由可信计算组织（Trusted Computing Group，TCG）来制定。目前 TPM 已经应用到大多数商用计算机、服务器和个人计算机。针对 TPM，2003 年 TCG 颁布了 TPM 1.2 规范。TPM 1.2 总体上是成功的，但也存在一些问题。例如适合 PC 平台，不适合服务器平台和嵌入式平台；只配置公钥密码，没有对称密码；哈希函数的设置存在一些问题；密码方案不支持本地化，世界各国应用困难；密钥和证书种类繁多，管理困难。

为解决这些问题，2014 年 TCG 推出 TPM 2.0 规范。2015 年 TPM 2.0 规范成为 ISO/IEC 国际标准。 TPM 2.0 改进了 TPM 1.2 的一些不足，如密码算法多样化、支持密码算法本地化（支持中国商用密码算法）、支持虚拟化、统一授权框架、增强了健壮性，从而为 TPM 的应用建立了更好的生态环境。

TPM 2.0 被称为下一代的 TPM。然而目前有关 TPM 2.0 的介绍资料非常少，广大科技工作者迫切需要一本介绍 TPM 2.0 的书籍，为此，机械工业出版社引进了本书。

本书是一本介绍 TPM 2.0 的技术专著，涵盖了 TPM 2.0 新特性以及如何使用 TPM 2.0 构建安全解决方案。书中既介绍了 TPM 2.0 及其设计原理，又介绍了 TPM 2.0 的基本功能、可信软件栈 TSS 2.0 以及如何编写代码通过 TSS 调用这些功能，同时还提供了相关范例，并介绍了利用 TPM 2.0 在新安全时代解决实际问题的技术方案。

本书的作者都是可信计算领域的著名专家，他们参与了 TCG 规范的制定，其中第一作者 Will Arthur 是英特尔公司资深固件工程师。他领导了英特尔可信执行技术（Intel TXT）中服务器端认证代码模块（ACM）的开发，并编写了 TCG TPM 2.0 系统接口、TPM 2.0 TAB 和资源管理规范。第二位作者 David Challener 目前是 TCG TPM 工作组的联合主席，

之前曾担任过 TSS 工作组、TCG 技术委员会和董事会的主席。

本书最大的特点是简明实用，既可以作为信息安全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。

本书由武汉大学王鹃、余发江、严飞、张立强、石源等翻译，武汉大学张焕国、赵波，英特尔公司李彦、姚颉文、龙勤、魏刚，国民技术公司刘鑫，华为公司李金明，大唐高鸿信息技术有限公司郑驰等审校。洪智、张雨菡、文茹、汪昕晨、胡威、樊成阳、李弈、李江琪、何能斌、张浩喆、马佳慈、王杰也参与了部分翻译和书稿整理工作。

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

2017 年 7 月

关于作者 *About the Author*

Will Arthur 是英特尔公司数据中心工程组的资深固件工程师。他领导了英特尔可信执行技术（TXT）中服务器端认证代码模块（ACM）的开发。作为一名活跃在可信计算组织的 TPM 和 TSS 工作小组的参与者，他编写了 TCG TPM 2.0 系统接口、TPM 2.0 TAB 和资源管理规范，开发了 TCG 版本的代码并实现了这些规范，审查并校订了 TPM 2.0 规范的可读性和准确性。Will 在底层嵌入式固件和软件开发方面拥有超过 30 年的工作经验，并且最近的 19 年一直在英特尔公司工作。Will 在亚利桑那州立大学获得了计算机科学学士学位。

David Challener 自十多年前起就致力于可信计算方面的工作。目前他是 TPM 工作组的联合主席，之前曾担任过 TSS 工作组、TCG 技术委员会和董事会的主席。他还为很多其他 TCG 规范做出过贡献。他拥有伊利诺伊大学应用数学博士学位，目前就职于约翰霍普金斯大学应用物理实验室。

About the Reviewers 技术评审人

Justin D. "Ozzie" Osborn 是约翰霍普金斯大学应用物理实验室的商业设备运营组的首席科学家。他在软件逆向工程和嵌入式软件开发方面有近十年的工作经验。他曾参与了涉及 TPM 软件开发和对 TPM 解决方案的漏洞分析的项目。

Monty Wiseman 是英特尔数据中心集团（DCG）的安全架构师。他目前参与的项目包括 TCG 架构、Intel TXT 技术、启动保护以及其他与安全相关的项目。Monty 参加并领导了 TCG PC 客户工作组和 TPM 1.2 安全评估工作组。他还参加了 TPM 和其他 TCG 工作组，并且是英特尔在 TCG 技术委员会的代表。Monty 在桌面、网络和大型机环境中拥有 20 年的工作经验，并在 Novell、Fujitsu 和 Control Data 公司中担任安全及其他技术职位。自 1975 年以来，他一直从事从大型机到微型计算机的硬件和软件开发。

前　言 Preface

“太有创造力了！”

“这本书太吸引人了！在读完最后一页之前我实在没法放下它。”

“我读得精疲力尽，连续三晚上熬夜看这本书，我的安眠药呢？”

“书里的悬念太折磨人了，我必须得把它们读完！”

如果你读完本书有上述评价，那么我们会非常高兴。然而对于任何一本数字安全方面的书籍，能够得到上述评价都会令人怀疑。数字安全相当于计算机的灾害保险。很少有人会关注它，并且人们通常不喜欢为它花钱直到灾难真的发生。到了那个时候，人们才会庆幸做好了准备或是为没有防范而难受。

也许，我们听上去像不停地叫着“天塌啦，天塌啦”的“四眼仔”，但是请一定要记住我们的话：数字安全的灾难正在降临。我们可以举出一大堆数据来证明数字安全威胁正在不断增加，但是也许你已经听过这些，并且，实话实说，你毫不在乎，至少是不够在乎。估计在这样的灾难对你个人产生影响之前，任何形式的说教都不能引起你的关注。

当你的声誉受到损害，财务受到影响，身份被盗，身体健康受到威胁，贵公司的声誉和财务受到损害时，你才意识到网络安全的重要性，但是那时可能已经太晚了。就像生活在洪泛区的人们，对于他们来说，洪水是否来临已经不是问题，关键在于灾难来临时，是否准备好了如何应对。而现在正是购买数字安全保险的时候！不要等到洪水来袭。

本书可以作为数字安全保险策略的一部分。TPM 被设计为数字安全解决方案的核心构件之一。在 2013 年 11 月给美国总统的“立即加强国家网络安全”的报告中建议“普及采用一个能够提供基本安全功能并遵循工业标准的微芯片（Trusted Platform Module，TPM），该芯片可以为手机和计算机提供加解密的基本安全功能。嵌入了 TPM 芯片的计算机和设备能够创建加密密钥并进行加密，并且只能由 TPM 进行解密。TPM 提供了高级网络安全所需要的有限但基本的功能。今天许多笔记本电脑和台式机中都具有 TPM 芯片。这些芯片被企业用于安全磁盘加密等任务，但它们尚未在智能手机、游戏机、电视机、车载计算机系统以及其他计算机设备和工业控制系统中大量应用。而这些系统需要使用 TPM，因为这些设备将会成为日益互联的设备生态系统的组成部分。”

本书的目的是鼓励年轻一代 IT 经理、安全架构师、系统程序员、应用程序开发人员和一般用户使用 TPM 作为越来越复杂的安全问题解决方案的基石，从而阻止针对个人及其雇主、国家机构的信息安全威胁的进一步加剧。同时，TPM 也是一个很酷的工具。有很多工程师像孩子一样利用 TPM 玩着简单的加密技术。这种向朋友发送加密消息的能力很吸引人，正如人们年轻的时候被间谍游戏吸引一样。并且，除了乐趣之外，TPM 的另一个吸引人之处在于可以利用它来保护自己的私有数字财产不被侵犯。

TPM 2.0 技术可以实现上述这些目标。我们相信这项技术，并希望读者也成为 TPM 2.0 的拥护者。希望你也会对这项技术感到兴奋，并且正如英特尔的创始人之一 Robert Noyce 所说的："利用它去做一些更棒的事。"

为什么选择这本书

技术规范通常是很差的用户手册，TPM 2.0 规范也不例外。一位技术规范的读者甚至认为它是"因难于理解而安全"的。

尽管规范企图尽可能清楚地描述功能，但其主要目标是描述 TPM 应如何工作，而不是如何使用它。它是针对 TPM 的实现者编写的，而不是为使用 TPM 的应用程序开发者。

另外，不管怎样，TPM 指令的详细操作是用 C 语言源码描述的。在 C 语言中数据结构使用各种关键字和修饰符来定义，这些关键字和修饰符允许将 Word 文档解析成 C 的头文件。 Microsoft 与 TCG 对规范中的源码颁发了开源许可证，这些源代码可用于实现 TPM。尽管 C 语言可以非常准确地描述操作行为，但代码的可读性总是比文本差。本书的主要目的之一就是对规范进行解读，让开发人员能更好地理解，尤其是那些需要了解规范的底层细节的开发人员。

许多读者不需要了解 TPM 的详细操作，他们只是想知道如何使用 TPM 的各种功能，以便利用这些功能开发新的安全应用。这些读者希望 TCG 软件栈（TCG Software Stack，TSS）可以隐藏底层的处理细节。因此，本书主要介绍如何使用 TPM，以及 TPM 的工作原理。在本书中，TPM 的特性会通过一些用例来描述。这些用例虽然不是非常全面，但它们描述了 TPM 2.0 规范中主要的功能。TPM 2.0 规范的内容非常丰富，除了这些用例之外，还可以用来实现一些其他的功能。

本书读者对象

在撰写本书时，我们想要努力吸引众多的读者群体：底层嵌入式系统开发人员、驱动程序开发人员、应用程序开发人员、安全架构师、工程管理人员，甚至一些安全领域的非技术用户。我们鼓励人们尽可能地广泛使用 TPM。

非专业的读者可着重关注介绍 TPM 的章节，包括 TPM 的历史（第 1 章）、基础安全概念（第 2 章），以及现有的 TPM 应用程序（第 4 章）。如果你不是专业程序员，但是有明确的安全需求，那么通过这几章对 TPM 的介绍，可以知道 TPM 的基本使用方法，从而设计

更多的新安全应用。

工程管理人员可以根据自己的需求和技术专长，按照自己的方式对 TPM 进行深入研究。我们也希望企业高层管理者可以读一读这本书，了解 TPM 提供的优势，对 TPM 相关的项目进行资助。例如，当他们意识到：利用 TPM，一个 IT 公司可以在允许所有设备接入网络之前对它们进行安全性识别；TPM 中的真随机数生成器可以产生系统获取随机数函数的随机种子；TPM 设计中内嵌的抗字典攻击保护功能可以帮助增强原本较弱的密码口令。企业高管可能会决定提供这些功能，让公司的每个人都来使用。

安全架构师必须要了解 TPM 2.0 的功能，并根据正在开发的应用，深入了解 TPM 的工作原理，以知道它所能提供的安全保证。同时，他们可以利用 TPM 的功能连接不同的设备和接口来实现可信的软件与网络。

应用程序开发人员，无论是架构师还是实现者，都需要重点关注这本书。这些读者需要从高层次的角度了解 TPM，并着重研究 TPM 的用例。TPM 2.0 的功能丰富，本书描述的用例希望能够激发你开发新的安全应用程序。开发人员不仅需要知道正确使用 TPM 所带来的安全保障，还必须知道对称和非对称密钥的基础知识以及在应用程序开发中使用的哈希函数，当然，他们不需要了解这些密码算法的细节。

我们也希望这本书对嵌入式系统开发人员、中间件开发人员和将 TCG 技术集成到操作系统及引导代码中的程序员有用。TPM 现在公开了更多的通用加密功能，当一般的加密库由于资源限制或许可权问题无法使用时，使用 TPM 的加密功能将是一个更好的选择。本书提供的内容对于底层开发人员已足够深入，可以满足他们的需求，并且可以用作解释规范的关键工具。为此，我们使用了图表以及代码实例来解释相关的概念。我们希望随着技术成本的降低（密码运算集成到嵌入式软件中的成本降低）以及对嵌入式软件攻击的加剧，嵌入式系统中将越来越多地使用 TPM。

本书的组织结构和内容

如果你刚开始学习安全方面的知识，或者需要对基础知识进行复习，第 2 章对理解本书所需要了解的基础知识进行了介绍。该章提供了密码学的高级知识：我们解释了对称和非对称密钥、安全哈希算法，以及如何使用消息验证码（MAC）来作为对称密钥数字签名。该章只是简单介绍用于实现加密算法的数学知识，因为本书不是一本一般用途的安全或密码学教科书，而且大多数 TPM 2.0 开发人员不需要掌握这些深奥的数学知识。

第 3 章介绍了 TPM 2.0 及其设计原理。该章首先介绍了 TPM 1.2 的应用程序和用例，这些应用程序和用例也适用于 TPM 2.0。接着，该章描述了 TPM 2.0 规范提供的新功能。该章可以帮助你了解为什么人们对这项技术感到兴奋并希望在自己的应用程序和操作环境中使用它。

第 4 章描述了使用 TPM 的现有应用程序（目前大多是基于 TPM 1.2 的）。假设这些应用程序中的大部分将被移植到 TPM 2.0。其中，一些是开源程序；一些是学术研究组织编写

的用于验证 TPM 功能的演示代码；一些则在很早前就存在了，它们恰好可以用来使用 TPM 的某些特性；而另一些则是专门编写来使用 TPM 功能的通用程序。

第 5 章对 TPM 2.0 规范进行了高度的概括，对其中的关键部分给出了指引，并对如何使用规范给出了一些最佳实践。

第 6 章介绍了如何搭建和使用运行 TPM 2.0 代码示例的执行环境。

第 7 章介绍了可信软件堆栈（TSS）。之所以提早介绍这部分内容，是因为后续的代码示例使用了 TSS 的各个层。

第 8 章开始深入探讨 TPM 2.0 功能，并介绍了 TPM 2.0 实体：密钥、数据块和非易失性（NV）索引。

第 9 章讨论 TPM 的 hierarchy。

第 10 章着重介绍了 TPM 的密钥。

第 11 章介绍了 NV 索引。

第 12 章介绍了 PCR 和验证。

第 13 章是本书最深入的章节之一，如果你正在开发使用会话和授权的底层代码和系统，那么本章对你十分重要。

第 14 章讨论扩展授权。

第 15 章解释了密钥管理。

第 16 章介绍 TPM 的审计功能。

第 17 章介绍了解密和加密会话以及如何设置它们。

第 18 章描述了对象、序列和会话上下文管理以及资源管理器的基本功能。

第 19 章介绍了 TPM 启动、初始化和配置。在使用 TPM 时，这些会在使用密钥和会话之前发生，但 TPM 实体、会话是理解 TPM 初始化和配置的前提条件。因此我们在前 3 章之后包括了本章的内容。

第 20 章介绍了调试 TPM 2.0 应用程序的最佳实践。

第 21 章描述了可以使用 TPM 2.0 功能的高级应用程序。

第 22 章介绍了使用 TPM 2.0 设备作为安全解决方案的平台级安全技术。

需要的基础知识

尽管这是一本技术书籍，但是我们尽可能地假设读者是零基础的。代码示例使用的是 C 语言，有一定的 C 语言基础对阅读本书是有帮助的。但是，本书中绝大多数的概念都是独立的，因此本书的大部分内容对于非程序员来讲也是可以理解的。我们对安全概念进行高度概括，并尽最大努力使你能够理解书中的内容。

了解 TPM 1.2 和 2.0 规范对阅读本书会有帮助，但并非是必需的。我们希望你从 www.trustedcomputinggroup.org 上下载 TPM 2.0 规范，以便在阅读本书时参考。

致谢

非常感谢外部和内部评审人的贡献、编辑和建议：

- Ken Goldman 撰写了许多章节，并认真地检查了书中的技术性错误。
- Emily Ratliff 和 Jon Geater 为第 22 章的 ARM 和 AMD 部分提供了专业的知识和经验。Bill Futrall 也为第 22 章提供了相关资料。
- Paul England 、David Wooten 和 Ari Singer 帮助我们理解了规范。
- Paul England 帮助我们了解了 Microsoft 的 TPM 接口。
- Monty Wiseman、Justin Osborn、Alex Eydelberg、Bill Futral、Jim Greene 和 Lisa Raykowski 都对本书做了技术性评论。
- 来自英特尔的 Patrick Hauke 为我们提供了支持和指导。
- 感谢 TSS 和 TPM WG 成员的很多直接或间接的贡献。

Contents 目　录