第一图书网, tushu007.com

<<可信计算>>

图书基本信息

书名：<<可信计算>>

13位ISBN编号：9787111253006

10位ISBN编号：7111253000

出版时间：2009-1

出版时间：机械工业出版社

作者：（美）查利纳（Challener，D.）等　著，赵波　等译

页数：245

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

前言

目前，可信平台模块(TrustedPlatformModule，TPM)成为世界各大PC供应商积极推广的一类新产品。
《可信计算》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。
《可信计算》内容《可信计算》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《可信计算》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＇I?M提供安全解决方案，并讨论了如何编码实现。
《可信计算》介绍了＇YPM的基本功能以及如何编写代码通过标准TCG(1：rustedComputingGroup，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FPM能够实现的解决方案。
在《可信计算》的撰写过程中，几位作者正从事将TSS1．1规范扩展到TSS1．2规范的工作。
TSS1．2可以访问由TPM1．2提供的新功能，《可信计算》在第14章中介绍了＇YPM1．2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TPM1．2新功能的读者，可以将第14章纳入学习过程中。
《可信计算》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《可信计算》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。
《可信计算》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，BruceSchneier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，《可信计算》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，《可信计算》的所有篇章都会对你有所帮助。
读者群体《可信计算》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＇YPM功能的代码，那么整《可信计算》都是有价值的。
如果想了解＇rPM的设计及其本质，就需要重点研究第一部分和第二部分。
《可信计算》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《可信计算》介绍了所有与＇FPM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，《可信计算》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＇FPM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TPM1．1编写程序，请阅读第4到10章。
如果想使用TPM1．2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。
《可信计算》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《可信计算》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。

第一图书网, tushu007.com

适用于可信计算爱好者如果读者考虑使用TPM，请参阅第l一3章和11一13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，《可信计算》(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!《可信计算》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＇TPM1．1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《可信计算》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TSSAPI。
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TSSAPI示例程序，可以区分1．1API和1．2API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。

第一图书网, tushu007.com

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．——IV2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TSS1．1到TSS1．2TSS12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TPM1．2的客户端匕运行。
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ATPM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BTSS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《可信计算》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《可信计算》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《可信计算》的评阅者提出许多宝贵的修改意见，他们是：DavidGrawrock、KenGoldman、SeanSmith和EmilyRatliff等。

第一图书网, tushu007.com

<<可信计算>>

内容概要

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，并讨沦了如何编码实现。
本书介绍了TPM的基本功能以及如何编写代码通过标准TCC(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。

第一图书网, tushu007.com

作者简介

David Challener美国伊利诺伊大学厄巴纳一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，加人Lenovo公司。
此后，作为Lenovo公司的代表加入TCG技术委员会、TP

第一图书网, tushu007.com

<<可信计算>>

书籍目录

第一图书网, tushu007.com

<<可信计算>>

章节摘录

插图：第一部分 背景材料第1章 可信计算概述本主主要描述由可信计算组织（TrustedComputingGroup,TCG）定义的可信平台模块(TrustedPlatformModule,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。

第一图书网, tushu007.com

<<可信计算>>

编辑推荐

目前，TPM(可信平台模块)成为世界各大PC供应商积极推广的一类新产品。
《可信计算》是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。
《可信计算》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。
书中介绍了TPM的基本功能以及如何编写代码通过标准TCG(Trusted Compting 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。
《可信计算》主要特点TPM提供的服务和功能。
TPM设备驱动程序：在BIOS中运行代码的解决方案、新操作系统的TSS栈和内存受限的环境。
· 使用TPM增强PC启动序列的安全性。
· 深入探讨密钥管理方面的问题：创建、存储、加载、迁移和使用密钥，对称密钥等。
· 将PKCS#11与TSS栈结合起来，以支持具有中间件服务的应用。
· TPM和隐私——包括如何避免隐私问题。
· 从TSS 1．1规范转移到TSS 1．2规范。
· TPM和TSS命令参考以及完整的函数库。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com