特色专业

普通高等教育信息安全类国家级特色专业系列规划教材

可信计算技术原理与应用

邹德清　羌卫中　金　海　编著
张焕国　主审

科学出版社

内 容 简 介

本书讨论可信计算的相关原理及应用，介绍国际可信计算组织(TCG)和中国可信计算联盟的可信计算相关知识，以及理论基础、技术规范、技术原理、编程和实践应用相结合的内容，同时引入最新的研究成果等。

全书总体上分为三大部分："背景知识"部分阐述可信计算相关的概念、密码学基础知识、可信计算组织(TCG)的核心规范，以及中国可信计算联盟的相关规范；"可信计算架构及功能"部分是本书的核心内容，介绍可信计算模块(TPM)的核心功能、动态可信度量根、可信启动、TCG的软件栈(TSS)及其接口函数、TSS的编程实例、国内可信密码模块(TCM)核心功能及其服务模块功能；"可信计算平台"部分介绍可信计算机技术及可信计算平台等。

本书可作为高等院校工科信息安全类专业的专业基础课教材，也可作为从事可信计算技术的科技人员的参考书。

图书在版编目(CIP)数据

可信计算技术原理与应用/邹德清，羌卫中，金海编著. —北京：科学出版社，2011

(普通高等教育信息安全类国家级特色专业系列规划教材)

ISBN 978-7-03-030357-8

Ⅰ.①可… Ⅱ.①邹…②羌…③金… Ⅲ.①计算机安全-安全技术-高等学校-教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2011)第027533号

丛书策划：匡 敏 潘斯斯

责任编辑：潘斯斯 张丽花/责任校对：刘小梅

责任印制：张克忠/封面设计：迷底书装

科学出版社出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京华正印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2011年5月第 一 版 开本：787×1092 1/16

2011年5月第一次印刷 印张：14 1/4

印数：1—4 000 字数：330 000

定价：30.00元

(如有印装质量问题，我社负责调换)

《普通高等教育信息安全类国家级特色专业系列规划教材》
编 委 会

前　言

伴随着现代计算机系统的发展，软件攻击变得更加复杂和自动化，传统安全防范手段的被动性以及软件自身的固有缺陷不足以应付日益增多的计算机安全威胁，单纯依靠软件的安全机制已经不能充分保护信息的安全。可信计算为克服上述安全问题提供了一个新的思路，为平台提供安全增强的硬件基础，并在这样的平台上通过软硬件结合的方式构建可信计算环境。可信计算环境确保其上进行的计算具有真实性、机密性和可控性等特性。利用可信计算环境提供的这些特性可以弥补仅依靠软件安全防范方式带来的不足，从而更好地解决计算机安全面临的问题和挑战。

可信计算组织(Trusted Computing Group，TCG)用实体行为的预期性来定义“可信”：如果一个实体的行为总是以预期的方式，朝着预期的目标，则该实体是可信的。我国计算机领域的资深专家沈昌祥院士对 TCG 可信计算的概念进行了扩展，他认为：可信要做到一个实体在实现给定目标对其行为总是如同预期一样的结果，强调行为结果的可预测和可控性。结合权威组织和专家的建议，在本书中可信计算是指系统提供的计算行为能够满足需求者对计算的期望，并且系统具有能够证明其计算可信性的能力。可信计算将加密、解密和认证等基本的安全功能交由硬件芯片来完成，并确保芯片中的信息不能在外部通过软件随意获取，这也是构建可信的计算机设备以及建立可信的计算机通信的基础。综合来看，可信计算平台可以为建设安全体系提供更加完善的底层基础设施，并为需要高安全级别的用户提供更强有力的应用安全解决方案。

本书针对可信计算组织提出的可信计算模块(Trusted Platform Module，TPM)技术，从技术规范、技术原理、编程和技术应用等多个角度进行阐述。全书总体上划分为三部分，包括背景知识、可信计算架构及功能、可信计算平台。

第一部分是“背景知识”。为了辅助读者准确、清晰理解可信计算知识，分为三章进行介绍：第 1 章阐述可信计算相关的概念，如可信计算被提出的原因分析，可信计算的发展历史、概念、应用状况等，并结合中国的可信计算状况进行分析；第 2 章介绍可信计算相关的密码学基础知识，针对国际上的 TPM 技术及国内具有自主知识产权的可信密码模块(Trusted Cryptography Module，TCM)技术所涉及的哈希函数及加密算法，TPM 采用了 SHA-1 函数、RSA 公钥密码及 PKI 认证体系等，而 TCM 采用了 SM3 密码杂凑算法、SMS4 对称加密算法，以及 SM2 椭圆曲线密码算法等；第 3 章 TCG 规范着重介绍 TCG 核心规范(主要包括 TCG 体系结构和可信平台模块结构)、特定平台规范(包括可信 PC 客户端规范、可信服务台器规范和可信移动设备规范等)、可信存储规范和可信网络连接规范；中国可信计算联盟规范则主要介绍了可信计算密码支撑平台功能与接口规范。

第二部分“可信计算架构及功能”是本书的核心内容。第 4 章介绍可信计算模块的核心功能，包括安全度量和报告、远程证明、数据保护，以及密钥管理；第 5 章介绍动态可信度量根，它是 TPM 实现静态度量的一种延伸，需要 CPU 的支持；第 6 章介绍可信启动，主要根据 TPM 提供的安全度量功能来实现，另外，结合 Intel TXT 技术分析动态可信启动过程；第 7 章和第 8 章介绍 TCG 软件栈、TCG 编程接口及编程应用；第 9 章介绍国产的可信密码模块(TCM)的核心功能及服务模块。

第三部分为“可信计算平台”。书中的介绍并未局限在可信计算技术本身，同时增加了结合可信计算技术构建可信计算平台的内容，第 10 章从整个计算机的角度来阐述可信计算；第 11 章和第 12 章介绍两个有代表性的可信计算平台：基于 Turaya 的可信计算平台和虚拟化可信计算平台。

本书的内容兼顾了技术规范、技术原理及编程应用，并扩展到可信平台。同时，为了更好地推进国内可信计算技术的发展，本书也介绍 TCM 的规范及技术原理。由于 TCM 编程应用在目前阶段还不够成熟，本书将在未来改版中加入关于 TCM 规范和 TCM 编程应用的内容。另外，由于本书只针对计算机主板上的安全芯片，未来版本中也将加入其他硬件安全相关的内容。

本书的出版受到国家重点基础研究发展计划(973 计划)项目“计算系统虚拟化基础理论与方法研究”、国家自然科学基金面上项目“逻辑虚拟域中软件执行的可信确保机制研究”，以及国家信息安全特色专业建设项目的资助。另外，在本书编写过程中得到了华中科技大学“服务计算技术与系统教育部重点实验室”暨“集群与网格计算湖北省重点实验室”系统安全研究组多位研究生的大力协助，包括程戈、代炜琦、项国富、陈刚、李敏、郑伟德、陈宏武、杨凯、王圣兰、段培，他们为本书的最终完成做了大量的辛勤工作，在此表示感谢！

我们在编写本书的过程中力图精益求精，但难免存在疏漏之处，敬请大家指正和谅解。

编　者

2010 年 11 月

目　录

第三部分　可信计算平台

第一部分　背景知识

第1章　可信计算概述

1.1　安全威胁

随着信息技术的发展，现代社会越来越依赖于计算机系统。特别是近年来，在互联网技术的推动下，计算机越来越多地应用到社会政治、经济、教育和军事等领域中，使计算平台的安全性变得越发重要。然而，自从计算机问世以来，计算机安全问题就一直伴随着计算机的发展而存在。近年来，伴随着软件攻击工具的复杂化和自动化，软件漏洞发现的数目急剧增多，再加以用户移动性的增强，针对软件的攻击所造成的安全危害日趋严重。

软件安全漏洞产生的根源在于现代软件系统惊人的复杂性，如2008年10月发布的2.6.27版本Linux内核代码库的代码量已经超过了1000万行。Windows Vista系统则达到了5000万行，集成了19500个驱动程序。一个主流的UNIX/Linux或Windows应用系统都是由上亿行代码构成的。研究表明，典型的产品级软件每千行代码就会有一个与安全相关的漏洞。那么，可以推算，一个主流应用系统有可能隐藏了10万个以上的安全漏洞。

常见的软件漏洞威胁有跨站脚本攻击(XSS)、SQL注入、缓冲区溢出、恶意文件执行、不安全的对象引用、不安全的身份鉴别和加密存储等。这些漏洞的数目正急剧上升，由CERT提供的漏洞统计数据如图1.1所示，2000年至2008年间所报告的漏洞总数大致呈现了两年翻一番的发展趋势。

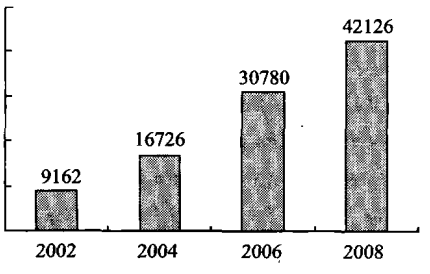

图1.1　CERT报告的软件漏洞统计数据

软件漏洞的泛滥为黑客提供了可乘之机。由于需要执行频繁的补丁更新，所以实际上大多数系统都存在或多或少的已知漏洞。由于缺乏有经验的管理员进行安全配置和补丁更新，与服务器系统相比较，客户端系统更容易受到攻击。IBM X-Force 2008安全报告指出黑客的注意力已经有从服务端向客户端转移的趋势。据初步统计，当今世界平均每20s就有一起黑客事件发生，仅在美国每年造成的经济损失就超过100亿美元。涉及政府机构、军事部门、科研院校和金融商业等部门的计算机犯罪严重干扰了人们的日常工作，也恶意侵犯了公民隐私，造成巨大的经济损失，甚至直接或间接地威胁到国家安全。

这些攻击导致存放在系统中的数据受到威胁。威胁来自多个方面：首先，个人或企业有价值的数据存在被电子盗窃的风险；其次，身份和鉴别信息的电子盗窃风险使得黑客能够进入其他的系统账户；另外，用户越来越移动化，因移动电子设备(笔记本电脑、掌上电脑和智能手机)失窃而造成的数据及身份信息泄露的风险也随之增加。根据赛门铁克的调查，由于计算机或其他的数据存储媒介的丢失造成的信息泄露占到了与身份相关的数据泄露的54%。图1.2显示了赛门铁克统计的公开报道的美国数据泄露案件持续增长的情况。

造成这种情况的重要原因是传统的安全防范方式的被动性和软件自身的固有缺陷，它们不足以应付日益增多的计算机安全威胁：第一，防火墙、入侵检测和病毒防范是构成传统信息安全系统的主要技术手段，这些技术手段是一种事后响应方式，即在攻击发生后或是进行中，通过对

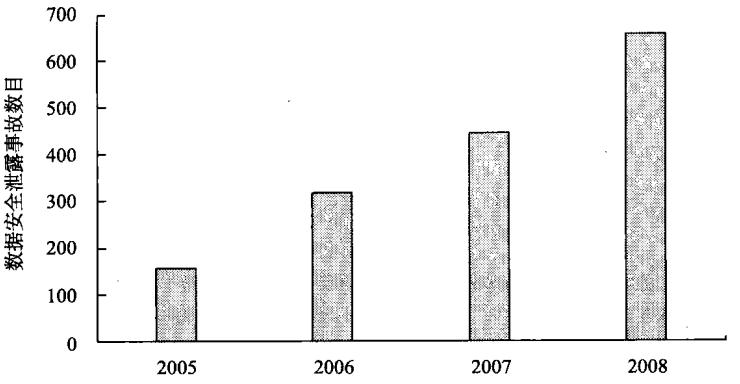

图 1.2　美国数据泄露统计

已发生过的滞后信息进行分析来判定是否存在攻击，从而进行相应的响应或防范。面对当今日趋复杂和变化多端的恶意攻击手段，这些传统防范手段往往无力应对新的攻击方式。第二，现有平台架构是开放式的，计算机资源可被用户任意使用，尤其是执行代码可任意修改。因此，在现有的软件架构下，恶意程序很容易植入到软件系统中。如果缺乏相关硬件的支持，仅仅依靠软件本身并不能完全检测出恶意代码，因为所有试图通过软件检测恶意代码的方法都无法证明检测软件自身是安全的。人们越来越意识到单纯依靠软件的安全机制已经不能够充分保护信息的安全。使用基于硬件的嵌入式安全解决手段已经成为一个重要的方向。

可信计算为克服上述安全问题提供了一个新的思路：为计算平台增加具有安全保护功能的硬件，使平台具有一定的物理保护能力，并在这样的平台上通过软硬件结合的方式构建可信计算环境。可信计算环境可以确保其上进行的计算具有某些特性，如使用可信计算环境保证其中运行程序和数据的真实性、机密性和可控性等。利用可信计算环境提供的这些特性可以弥补仅依靠软件安全防范方式带来的不足，从而更好地解决计算机安全面临的问题和挑战。

1.2　可信计算的发展历史

20 世纪 80 年代中期，美国国防部国家计算机安全中心代表国防部为适应军事计算机的保密需要，在 70 年代的理论研究成果“计算机保密模型”的基础上，制定并出版了“可信计算机安全评价标准(TCSEC)”。在 TCSEC 中，“可信计算机”和“可信计算基”(Trusted Computing Base，TCB)的概念第一次被提出来，而 TCB 被称为是系统安全的基础。1987 年 7 月，该中心又针对网络、系统和数据库提出了三个解释性文件，即可信网络解释(Trusted Network Interpretation，TNI)、计算机安全系统解释(Computer Security Subsystem Interpretation，CSSI)和可信数据库解释(Trusted Database Interpretation，TDI)，形成了安全信息系统体系结构的最早原则。1993 年 1 月，美国公布了融合欧洲 ITSEC 的可信计算机安全评价准则之联邦准则。

1997 年，W. A. Arbaugh 等在项目 AEGIS 中提出并实现了一个称为安全启动的体系结构。该文已经体现出“信任传递”的概念。计算机从启动的过程开始，由前一个程序度量后一个程序的完整性，只有在完整性通过验证后，才把控制权交给后一个程序，如此反复直到操作系统的启动。这种硬件保护软件机制的思想促使了可信计算的发展。

为了解决个人计算机结构上的不安全性，并从底层入手提高其可信性，几大 IT 公司 Com-

paq、HP、IBM、Intel 和 Microsoft 于 1999 年 10 月发起并组织了可信计算平台联盟(Trusted Computing Platform Alliance,TCPA),成员达 160 家。TCPA 定义了具有安全存储和加密功能的可信平台模块(TPM),并于 2001 年 1 月发布了基于硬件系统的"可信计算平台规范"(V1.0)。2003 年 3 月,TCPA 改组为 TCG(Trusted Computing Group),其目的是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台,以提高整体的安全性,扩展可信的范围。可信计算平台的涵盖范围是广泛的,如个人计算机、PDA、手机,以及其他的一些平台。随后,一些国际芯片厂商依照 TCG 规范实现了 TPM 芯片。

1.3 可信计算在中国

我国在可信计算技术研究方面起步较早。在安全芯片、可信安全主机、安全操作系统和可信计算平台应用等方面都先后开展了大量的研究工作,并取得了可喜的成果。早在 20 世纪 90 年代,国内有公司就开发了个人计算机安全防范系统,实现了可信防范,其结构和功能与 TCG 提出的可信计算平台类同。从 2000 年开始,国内的可信安全计算机的研发工作已经启动;2004 年,具有自主知识产权的可信计算机产品开始面市。

在国家密码管理局和国内 IT 企业的推动下,2002 年,中国信息产业商会信息安全产业分会成立,该分会提出了可信网络世界体系结构框架(Trusted Cyber Architecture Framework,TCAF)。TCAF 计划针对中国信息化的体系结构设计核心可信平台,并对体系结构与标准化方法的概念、模型、方法、定义、引用和分级进行描述与说明。2005 年 1 月,我国成立国家安全标准委员会 WG1 可信计算工作小组专门规划可信计算的相关标准。通过参照国外 TCG 规范,国家密码管理局联合国内一些研究单位及 IT 企业联合推出了可信密码模块标准,并于 2006 年颁布了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》。2007 年,由沈昌祥院士发起、10 余家单位共同参与,研究制定"可信计算平台密码规范"、"可信计算基础支撑软件"、"可信平台主机规范"和"可信网络连接规范"等草案,形成了可信计算标准系列的主体框架,解决了芯片、软件栈、主机平台和网络连接基本结构等主要问题。

TCM 和可信计算产品均基于国家密码算法,国家信息安全的自主事业也正是通过对该核心部件及其密码算法的自主控制与执行来实现的。作为构建中国信息安全的信任根,如同 DNA 一样,TCM 奠定了可信计算技术的安全根基。带有硬件 TCM 的可信计算产品在计算机体系结构上取得了突破,可以有效防止病毒恶意代码的攻击,保证用户的机密信息不被窃取,保障数据和系统不被非法破坏,从而构建安全可信赖的计算环境。有了标准的引导,芯片厂商和整机厂商就可以按照相应的密码规范、芯片规范和软件接口,搞好产品规划,研究设计方案,开发出相应的产品。2008 年 4 月底,中国可信计算联盟(CTCU)在国家信息中心成立,现已有 20 家正式成员,包含计算机厂商、信息安全厂商和一些应用厂商,也包括国家的科研院所。CTCU 的成立标志着中国在可信计算和信息安全领域进行了一次成功的尝试,标志着可信计算由理论逐步转化为产业,转入到实质性的实现阶段,并逐步开始应用到政府和军事等领域。

1.4 可信计算的定义

可信计算为解决计算机的安全问题带来了新的希望。然而,在中文计算机语境中,"可信"却有着不同的定义,在中文文献中使用最多的有以下几种。

可信计算组织(TCG)用实体行为的预期性来定义“可信”:如果一个实体的行为是以预期的方式符合预期的目标,则该实体是可信的。

ISO/IEC 15408 标准定义“可信”为:参与计算的组件、操作或过程在任意的条件下是可预测的,并能够抵御病毒和物理干扰。

我国著名的信息安全专家沈昌祥院士对上述定义进行了综合和扩展,他认为:“可信”要做到一个实体在实现给定目标时其行为总是如同预期一样的结果,强调行为结果的可预测和可控制。

其他的一些解释还有:“可信”是指计算机系统所提供的服务可以被证明是可信赖的;如果一个系统按照预期的设计和策略运行,这个系统是可信的;当第二个实体符合第一个实体的期望行为时,第一个实体可假设第二个实体是可信的;可信≈安全+可靠,可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统等。

从中文语义上看,这些定义是混乱的,甚至是自相矛盾的。例如,按照 TCG 的定义,一个恶意软件在预期时间内做出了期望的危害行为,那么它是可信的;依照 ISO/IEC 15408 标准定义却是不可信的。实际上,上述的定义都是正确的,是对“可信”从不同的方面给出的定义。

“可信”是一个很复杂的概念,而且各个不同领域的研究者对此也有不同的定义,这一概念长期存在于人类社会中,但是计算机科学领域对“可信”的研究才刚刚起步,并且大多借鉴了心理学、社会学和经济学等科学研究领域的成果。不同领域的研究者在研究上各有侧重点,有些强调“可信”的形式化描述,有些强调“可信”的特征研究,有些强调“可信”在实际系统中应用研究,这就造成了“可信”定义的多样化,有的甚至是相互冲突的。

如果追溯上述“可信”定义的起源,可以看到这些定义对应着以下三种不同的研究背景:可信赖计算(Dependable Computing)、安全计算(Security Computing)和信任计算(Trusted Computing)。可信赖计算源自早期的容错计算:主要针对元器件、系统和网络,对包括设计、制造、运行和维修在内的全过程中出现的各种非恶意故障进行故障检测、故障诊断、故障避免和故障容忍,使系统达到高可靠与高可用。安全计算主要针对系统和网络运行过程中的恶意攻击,和可信赖计算相比,不同之处在于它针对的故障不同,安全计算主要针对的是人为的恶意攻击,而可信赖计算是针对的是非恶意的攻击。信任计算源自早期的安全硬件设计,基本思想为:假定真实性可以用于度量并且不考虑度量中的损失,给出了一个“可信”在实体间传递的方法——在计算机系统中首先建立一个信任根,再建立一条信任链,一级度量认证一级,一级信任一级,把信任关系扩大到整个计算机系统,从而确保计算机系统可信。

可信赖计算、安全计算和信任计算在研究内容上有一定的交叉,并且国内的不少文献都将 Dependable Computing 和 Trusted Computing 统一翻译成“可信计算”。广义上的“可信计算”应该包括“可信赖计算”、“安全计算”和“信任计算”,而本书的“可信计算”侧重于 TCG 及沈昌祥院士给出的定义,即为 Trusted Computing。

1.5 可信计算的应用

可信计算平台将加密、解密和认证等基本的安全功能交由硬件芯片来完成,并确保芯片中的信息不能在外部通过软件被随意获取。在这种情况下,除非将硬件芯片从系统中移除,否则理论上是无法突破这层防护的,这也是构建可信的计算机设备,以及建立可信的计算机通信的基础。在硬件层执行保护的另外一个优势是能够获得独立于软件环境的安全保护,这就可以设计出具有更高安全限制能力的硬件系统。

通过硬件芯片执行相对基础和底层的安全功能，能保证一些软件层的非法访问和恶意操作无法完成，同时这也为生产更安全的软件系统提供了支持。综合来看，可信计算平台可以为建设安全体系提供更加完善的底层基础设施，并为需要高安全级别的用户提供更强有力的应用安全解决方案。

对于安全要求较高的场合，可信计算平台能够为用户提供更加有效的安全防护。在应用了可信计算技术之后，无论是要保护私密性数据，还是要控制网络访问，以及系统可用性保障等，都能够获得更高的保护强度。下面以个人计算机平台为主线来了解一下目前流行的可信计算应用，这些应用包含了可信计算应用最广泛的加密领域、作为软件系统核心的操作系统领域，以及网络传输控制和安全管理领域等方面的内容。

1.5.1 应用领域：信息加密保护

即使可信计算平台成为主流，加密仍将是安全保护方面的核心力量，只是应用 TPM 将使系统的加密更具可信性。IBM 是最早利用可信计算技术保护计算机设备的厂商之一，针对个人计算机市场推出的解决方案被称为 IBM 嵌入式安全子系统，该系统与 TPM 规范兼容。

这个安全子系统由内嵌在计算机中的安全芯片和 IBM 专用的客户端安全软件组成。安全芯片可以应用于登录密码、加密密钥和数字证书的保护，同时也可对文件系统（利用 IBM 的文件和文件夹加密功能）和网络传输进行加密。

由于安全芯片可以在 200ms 内完成 RSA 运算，所以系统的运行并不会受到明显的影响。除了这些保护功能之外，该安全系统的一个突出优点是能够防止计算机内的数据被非法获取。事实上，在没有安全子系统口令的情况下未获授权的用户是无法获取系统中任何信息的，因为用户在离开安全芯片的情况下无法读取硬盘中的数据。

安全芯片内部的信息存储和传送也经过了高强度的加密，加之 IBM 采用了特殊的芯片封装方法，使得安全芯片的破解极其困难。正确地应用安全子系统之后，用户的数据可以得到妥善的保护，即使在失窃的情况下用户的信息也不会泄密。另外，用户也要注意牢记该系统的口令信息，用户一旦被自身的系统锁在外边时往往会意识到这种系统的安全。

除了 IBM，HP 也有类似的产品；在国内，武汉瑞达和联想都推出了相似的产品。武汉瑞达是中国最早开始可信计算研发的公司之一，已经形成了全套自主知识产权的软硬件环境。瑞达推出的可信计算机产品包含了多种安全功能，如插入特别的电子钥匙或 IC 卡才能开启计算机，为计算机提供唯一的标识，控制所有文件的输入输出等。联想借其推出的“恒智”安全芯片成为继 ATLEM 之后全球第二个推出符合 TPM 1.2 规范安全芯片的厂商。“恒智”芯片可用于系统完整性校验，并能够标识计算机身份以防止冒用，而且该芯片将所有密钥信息都存储在其中，安全性大大提高。

1.5.2 应用领域：操作系统安全

虽然 TCG 所推出的规范大部分针对硬件设施，但是同样有一些针对软件层的规范，其中应用较多的一项技术是微软加密文件系统（EFS），这是微软向操作系统中集成可信计算技术的最早尝试之一，Windows 2000 及之后出现的 Windows XP 等系统都支持该特性。

在微软操作系统 Windows Vista 中，一个全新的被称为安全启动的特性将被应用，这是 Windows 所应用的第一个基于硬件的安全方案。一个符合 TPM 规范的硬件设备将对每个 Windows 系统开机时需要用到的文件进行标记，在开机的过程中一旦检验出标记状态不符合，

就很可能意味着系统受到了非授权的篡改或破坏。

这种保护机制的问题在于如果由于用户的疏忽或者应用软件的问题造成文件损坏，也可能使标记不符，这将对用户的使用造成不小的困扰。

1.5.3 应用领域：网络保护

3Com 公司提供集成了嵌入式防火墙(EFW)的网卡产品，用以向安装了该产品的计算机提供可定制的防火墙保护，另外还提供硬件 VPN 功能。由于支持基于 TPM 规范的认证，用户能够利用这类网卡执行更好的计算机管理，使得只有合法的网卡才能访问企业网络。

对于执行了较严格策略的网络来说，即使是非法用户使用失窃的网卡同样无法连入到企业网络中。通过将防范和管理手段更加有效地部署到终端，这类嵌入式防火墙产品使用户可以建立更具可信性的网络。网卡中的硬件防火墙模块相对于每个终端计算机上安装的软件防火墙来说性能更好，终端往往要为软件防火墙耗费很多的运算能力。

不过，嵌入式防火墙的可配置能力和可扩展能力要相对差些。如果用户不需要太过复杂的防火墙规则，并且希望更好地控制网络访问，那么利用这种形式的产品将会非常有效。

1.5.4 应用领域：安全管理

Intel 主动管理技术(AMT)是为远程计算机管理而设计的。之所以将其划归为可信计算技术是因为这项技术对于安全管理来说具有非常独特的意义和重要的作用，而且 AMT 的运作方式与 TPM 规范所提到的方式非常吻合。

在支持 AMT 的处理器、主板芯片组和网卡的计算机系统当中，即使在软件系统崩溃、BIOS 损坏，甚至是没有开机的状态下管理员仍然能对计算机完成很多远程操作。

举例来说，在系统因病毒而瘫痪的情况下，管理员可以利用 AMT 技术进行远程病毒清除、补丁更新乃至操作系统安装等工作，从而极大地提高安全事件的响应速度并降低管理成本。执行更加复杂的管理工作依赖于软件环境的支持，目前已经有很多计算机管理解决方案的厂商开始在其产品线中支持 AMT。

在新的解决方案中，用户无须在终端计算机中部署任何客户端程序，而只通过 AMT 即可完成多种复杂的管理功能。AMT 在系统可用性上还有很多的贡献，想象一下在支持 AMT 的网卡中写入一些服务功能，这样在计算机系统失效的情况下这些服务仍将能够执行。

1.6 现状与挑战

本节将先对可信计算目前的状况及未来的发展趋势进行分析，并提出其所面临的问题和挑战。

1.6.1 可信计算的现状思考

可信计算的目的是通过软件和硬件相结合的方式使其上进行的计算具有某些特性，并利用这些特性来弥补仅依靠传统安全防范方式的不足，从而更好地解决计算机安全面临的挑战和问题。尽管无论从理念上还是实效上来说可信计算平台都有所创新，但可信计算并不等同于绝对安全，不能解决所有的安全问题。可信计算只是提供了一种加强系统安全的方式，能够结合传统的安全技术来增强系统的安全性。但是，“没有绝对的安全”这一规律并不会因为可信计算平台的普及而失效。可信计算平台只是提供了一个支点，至于是否能够使之发挥作用还要依赖实际

的实施者。

不良的产品设计很容易导致安全问题。尽管基于硬件的 TPM 安全性很高，但是一旦发现安全问题，攻击者会以此控制计算机系统。由于目前的可信计算通常需要与相应的软件结合起来工作，不正确的软件使用或密码管理不善都可能为可信计算平台带来安全威胁。

安全系统的融合性与联动性一直是困扰信息安全产业的一个难题，可信计算成功地在终端层次上取得了突破，如何将可信计算延展到更深更广的层面上以建立起更具安全性的计算设施呢？事实上，“以更高的目标建立更加抽象的可信计算架构”是有志于在信息安全行业获得领先地位者所给出的答案。比之可信计算平台，可信网络架构在更高的抽象层次上和更广的作用范围内为信息安全的发展提供了指导。如果可信网络架构能够形成相对统一的标准并获得切实的应用，那将对全球的信息安全建设起到积极的推动作用。

在评估一项新技术时，可以从这样一个角度来判定其地位：该技术是否能够全面替代旧有的技术。从实际的情况出发可得出结论：可信计算平台在创新的同时仍然着力于增强已有安全体系。传统的安全防范体系和方法并不会因为可信计算平台的出现而消失。在未来的很长时间里，可信计算平台与非可信计算平台将互相融合，并朝着更加安全的系统形式的方向发展。

1.6.2 机遇和挑战

信息安全对国家安全的重要性不言而喻，甚至可以说，信息安全在今天已经能够影响国家安全的全局，在电子政务、政府、军队、科研等领域有着广泛的应用。在这种情况下应运而生的可信计算有广阔的发展前景，因为这种技术对于普通用户，以及金融、政府、军队等领域来说，能从硬件结构上为计算平台构建安全体系，试图从根本上解决当前存在的安全难题，并带给计算应用更高的安全性。

然而，可信计算的发展还存在着众多的问题，如理论研究相对滞后，无论是国外还是国内，可信计算的理论研究落后于技术开发。至今，尚没有公认的可信计算理论模型。可信测量是可信计算的基础，但是目前尚缺少软件的动态可信性的度量理论与方法。信任链技术是可信计算平台的一项关键技术，然而信任链的理论，特别是“信任”在传递过程中的损失度量尚需要深入研究，需要把信任链建立在坚实的理论基础之上。

另外，还存有一些尚待攻克的关键技术，即国内外的可信计算机都没能完全实现 TCG 的技术规范，如动态可信度量、存储、报告机制，以及安全 I/O 等。而且，操作系统、网络、数据库和应用的可信机制配套的缺乏也影响着可信计算的发展。目前，TCG 给出了可信计算硬件平台的相关技术规范和可信网络连接的技术规范，但还没有关于可信操作系统、可信数据库、可信应用软件的技术规范。只有可信的硬件平台，没有可信的操作系统、网络、数据库和应用，整个系统还是不安全的。

➢思考题

1.1 概述当前软件系统具有哪些安全威胁？与传统的安全防范手段相比，可信计算在解决系统的安全方面具有何种优势？

1.2 概述可信计算的定义。

1.3 概述中国提出的可信计算标准和国际的可信计算标准的关键区别。

1.4 概述国内可信计算发展的历程。

1.5 概述可信计算的典型应用场景及其应用范例。

第2章　密码学基础

本章将针对 TPM/TCM 中采用的密码学基础知识进行介绍。

2.1　Hash 函数

Hash 函数又称为哈希函数、散列函数或杂凑函数，是密码体制中常用的一类公开函数。所谓 Hash 函数，就是将任意长度的消息映射为较短的固定长度的消息摘要。Hash 函数主要用于消息完整性检测和消息认证，常分为两类：强无碰撞的 Hash 函数和弱无碰撞的 Hash 函数。

强无碰撞的 Hash 函数 h 需要满足下列条件：

(1) h 的输出长度是固定的；

(2) h 的输入可以是任意长度的任何信息或文件 M；

(3) 给定 h 和 M，计算 $h(M)$ 是容易的；

(4) 给定 h 和一个随机选择的 Z，寻找消息 M，使得 $h(M)=Z$，这在计算上是不可行的，这一性质称为函数的单向性；

(5) 给定 h，找两个不同的信息 M_1 和 M_2，使得 $h(M_1)=h(M_2)$，这在计算上是不可行的。

弱无碰撞的 Hash 函数 h 需要满足下列条件：

(1) h 的输出长度是固定的；

(2) h 的输入可以是任意长度的任何信息或文件 M；

(3) 给定 h 和 M，计算 $h(M)$ 是容易的；

(4) 给定 h 和一个随机选择的 Z，寻找消息 M，使得 $h(M)=Z$，这在计算上是不可行的；

(5) 给定 h 和一个随机选择的信息 M_1，找另一个不同的信息 M_2，使得 $h(M_1)=h(M_2)$，这在计算上是不可行的。

目前，Hash 函数被用于消息鉴别和数字签名系统中。将 Hash 函数用于数字签名中有很多益处。

(1) 可提高签名的速度：当需要的消息 m 过长时，可用 Hash 函数将 m 压缩成某一固定范围内的数据 $m'=h(m)$，然后再计算签名 $s=\mathrm{Sig}_k(m')$，其中，k 是签名密钥，Sig_k 是签名函数。

(2) 可以不泄露要签名的消息：对消息 m 的签名是 $s=\mathrm{Sig}_k(m')$，这里的 Hash 函数 h 是公开的，$m'=h(m)$ 也可以是公开的。根据 Hash 函数的性质，从 $m'=h(m)$ 中恢复出 m 几乎是不可能的，因此可以保密消息 m。

(3) 可以提高签名系统的安全性，有一些针对 RSA 等签名的攻击可以通过采用 Hash 函数后再签名来进行防范。

2.1.1　SHA 算法

1. SHA 算法概述

SHA 家族包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 这 5 个算法，后 4 个算法统