·计算机工程与应用·

可信计算及其进展

周明天[1]，谭 良[2]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 四川师范大学四川省软件重点实验室 成都 610066)

【摘要】详细介绍了“可信计算”的发展历程，总结了容错计算(可信系统与网络)、安全操作系统、网络安全等领域的研究对可信计算形成和发展的推动作用；提出了对可信计算的概念、研究对象、目的以及可信计算的体系结构的看法；综述了可信计算中的终端可信、终端可信应用、可信网络连接、可信网络服务、交易可信、可信评测和管理方法等方面的研究内容，并进行了分析和点评，结合已有的研究成果，展望了可信计算未来的研究方向及其面对的挑战。

关 键 词 信息安全; 网络安全; 可信计算; 终端可信

中图分类号 TP311 文献标识码 A

Progress in Trusted Computing

ZHOU Ming-tian[1], TAN Liang[2]

(1. School of Computer Science and Engineering, Univ. of Electron. Sci. & Tech. of China Chengdu 610054;
2. Software Key Lab. of Sichuan Province, Sichuan Normal University Chengdu 610066)

Abstract With the increasing application systems on Internet, the security problems grow day by day. However the traditional information security technology can't resolve the current complex security problems. So how to establish a trusted computing environment, which can be fit for the new generation information requirements, has been turned into one of the most important tasks in information technology domain. In this paper, the development history of the trusted computing is first introduced particularly, including Fault-Tolerant Computing (Dependable systems and networks), Security Operator System and Network Security, and so on. And then the concept, object, objective, and architecture of trusted computing are studied, The research aspects of trusted computing are addressed such as the trusted end–user, trusted end-user application, trusted network connection, trusted server, trusted transaction, and trusted evaluation and management. Based on the analysis to the shortcomings and problems of these techniques, the trend of the research and the application is discussed.

Key words information security; network security; trusted computing; trusted end-user

Internet及支撑它的不同信息技术网络构成了人类有史以来最为复杂的结构[1]，在迅速发展的过程中越来越深刻地影响着人们的日常生活。基于Internet的应用在社会各个领域越来越多地实现和开展，涉及金融、电信、宇航、电子商务、电子政务甚至军事。但是由于Internet天生的开放和动态特性导致其在安全和可靠方面的欠缺，越来越制约了基于Internet应用的发展，特别是电子政务和电子商务。如何结合应用需要，在开放的、动态的Internet环境下，实现可信的信息资源共享和协作，即如何为基于Internet的应用系统提供可信保障，构建新一代适应信息发展需求的可信计算环境，成为当前工业界和学术界密切关注和积极从事的重要课题[2-7]。

计算机学科属于计算科学，文献[8-10]对计算科学作了全面的回顾和展望。50多年以来，人们在计算科学、集成芯片、软件与人机交互等方面做了大量的研究工作，取得了大量的成果，使人类进入了一个高度发达的信息时代。目前，尽管计算科学还面临不少挑战，但已经发展到了一个比较成熟的阶段，因而可信需求才显得迫切而关键。美国国家科学基金会就提出了可信计算是计算科学进一步发展的需要[2]。

目前，可信计算得到了学术界和产业界的高度关注。在学术界，包括NSF[2]、一些大型跨国公司的研

收稿日期：2006－06－25

基金项目：国家863宽带VPN资助项目(863-104-03-01)；四川省科技攻关项目(03GG007-007)

作者简介：周明天(1939－)，男，教授，博士生导师，主要从事网络计算、信息安全、分布并处理方面的研究；谭 良(1972－)，男，博士，副教授，主要从事信息安全、中间件方面的研究.

究院、各国的研究机构和大学[11]、军事和国防机构等都掀起了研究热潮。在产业界，由Intel、Compaq、HP、IBM、Microsoft于1999年10月发起了一个“可信计算平台联盟”(Trusted Computing Platform Alliance，TCPA)[3-4]，并提出了“可信计算”的概念，力图利用可信技术构建一个通用的终端硬件平台。2001年1月TCPA发布标准规范(v1.1)，2003年TCPA改组为可信计算集团(TCG)[5-6]，成员迅速扩大为近200家，使得“可信计算”迅速遍及全球。

但是，按照惠特刊的观点[12]，可信计算还不是一个学科领域。因为按一个学科领域的要求，可信计算的很多基本问题都没有解决，诸如什么是可信计算；可信计算的研究对象和目标是什么；可信计算有什么样的体系结构；可信计算与其他相关领域有什么样的关系，等等。尽管研究可信计算的智力群体逐渐在全世界形成，并拥有一批该领域的权威和学术带头人，但是即使在这一智力群体内部，对可信计算的一些基本问题也还存在许多争议[13-20]。

1 可信计算的发展历程

可信计算的形成有一个历史过程。在可信计算的形成过程中，容错计算、安全操作系统和网络安全等领域的研究使可信计算的含义不断拓展，由侧重于硬件的可靠性、可用性，到针对硬件平台、软件系统服务的综合可信，适应了Internet应用系统不断拓展的发展需要。

1.1 容错计算阶段

在计算机领域，对于“可信”的研究，可追溯到第一台计算机的研制。那时人们就认识到，不论怎样精心设计，选择多么好的元件，物理缺陷和设计错误总是不可避免的，所以需要各种容错技术来维持系统的正常运行[21]。计算机研制和应用的初期，对计算机硬件比较关注。但是，对计算机高性能的需求使得时钟频率大大提高，因而降低了计算机的可靠性。随着元件可靠性的大幅度提高，可靠性问题有所改善。此后人们还关注设计错误、交互错误、恶意推理、暗藏入侵等人为故障造成的各种系统失效状况，研发了集成故障检测技术、冗余备份系统的高可用性容错计算机。

容错计算，作为计算科学的一个学科领域，文献[22]综述了它的形成和发展过程。1999年IEEE太平洋沿岸容错系统会议改名为IEEE可信计算会议，在香港召开。2000年IEEE国际容错计算会议(FTCS)与国际信息处理联合会(IFIP)10.4工作组主持的关键应用可信计算工作会议合并，并从此改名为IEEE可信系统与网络国际会议(ICDSN)[23]。“ICDSN'2000”当年在纽约召开，标志着容错计算领域的研究，无论在内容、方法和组织方面都有重大调整。2000年12月11日美国卡内基梅隆大学与美国国家宇航总署(NASA)的Ames研究中心为主成立了高可信计算联盟(High Dependability Computing Consortium)，包括Adobe、康柏、惠普、IBM、微软、Sybase、SUN在内的12家信息产业公司，麻省理工学院、乔治亚理工学院和华盛顿大学等都加入了该联盟[24]。成立大会由卡内基梅隆大学校长和Ames研究中心主任主持，并决定在宇航总署的加州硅谷研究园设立卡内基梅隆大学分校园，对高可信性计算进行基础研究、实验研究和工程研究，力图使计算机系统的建造和维护成为像土木工程、医学一样的学科。

值得注意的是，在容错计算领域，可信性被定义为计算机系统的一种性质，它所提供的服务是用户可感知的一种行为，并可以论证其可信赖[22,25]，而用户则是能与之互动的另一个系统(人或者物理的系统)。因为“可靠(Dependability)”而“可信”，因此容错计算又称为“可靠计算”(Dependable Computing)。容错计算领域的可信性包括可用性、可靠性、可维护性、安全性、健壮性和可测试性等。

1.2 安全操作系统阶段

实际上，从计算机产生开始，人们就一直在研究和开发操作系统，并将“容错计算”取得的成果应用于操作系统。从50年代中期出现的第一个简单的批处理系统，到60年代中期出现的多道程序批处理系统，以及此后的基于多道程序的分时系统，甚至再后来的实时系统和分布式操作系统[26]，仅仅靠“容错技术”并不能完全解决操作系统对共享资源的安全访问问题。

1967年，计算机资源共享系统的安全控制问题引起了美国国防部的高度重视，国防科学部(Defense Science Board)旗下的计算机安全任务组(Task Force on Computer Security)的组建，拉开了操作系统安全研究的序幕[27-28]。1969年，文献[29]发表了有关Adept-50安全控制的研究成果；同年，文献[30]通过形式化表示

方法，运用主体(Subject)、客体(Object)和访问矩阵(Access Matrix)的思想第一次对访问控制问题进行了抽象。1970年，文献[31]发表了对多渠道访问的资源共享的计算机系统引起的安全问题的研究报告。1972年，作为承担美国空军的一项计算机安全规划研究任务的研究成果，文献[32]提出了监控机(Reference Monitor)、验证机制(Reference Validation Mechanism)、安全核(Security Kernel)和安全建模(modeling)等思想，形成了对“Trusted”问题的研究。

在探索如何研制安全计算机系统的同时，人们也在研究如何建立评价标准，衡量计算机系统的安全性。1983 年，美国国防部颁布了历史上第一个计算机安全评价标准，这就是著名的可信计算机系统评价标准，简称TCSEC[33]，又称橙皮书。1985年，美国国防部对TCSEC进行了修订[34]。TCSEC 标准是在基于安全核技术的安全操作系统研究的基础上制定出来的，标准中使用的可信计算基(Trusted Computing Base，TCB)就是安全核研究成果的表现，与当前的“Trusted Computing”有极大的联系。

1.3 网络安全阶段

随着网络技术的不断发展和Internet的日益普及，人们对Internet的依赖也越来越强，互联网已经成为人们生活的一个部分。然而，Internet是一个面向大众的开放系统，对于信息的保密和系统安全考虑不完善。从技术角度来说，保护网络的安全包括两个方面的技术内容：(1) 开发各种网络安全应用系统，包括身份认证、授权和访问控制、PKI/PMI、IPSec、电子邮件安全、Web与电子商务安全、防火墙、VPN、安全扫描、入侵检测、安全审计、网络病毒防范、应急响应以及信息过滤技术等，这些系统一般可独立运用运行于网络平台之上；(2) 将各种与网络安全相关的组件或系统组成网络可信基(Network TCB)[35-8]，内嵌在网络平台中，受网络平台保护，与TCB受OS保护类似。从这两方面的技术发展来看，前者得到了产业界的广泛支持，并成为主流的网络安全解决方案。后者得到学术界的广泛重视，学术界还对“可信系统(Trusted System)”和“可信组件(Trusted Component)”进行了广泛的研究。1987年，美国国家计算机安全中心提出的可信网络解释(TNI1987)[38]就是这一技术的标志性成果。

当前大部分信息安全系统主要是由防火墙、入侵检测和病毒防范等组成。“堵漏洞、作高墙、防外攻”，但安全问题防不胜防。当前网络安全措施存在的两个缺陷[39]：一是只防外不防内；二是忽略了对终端的保护终端往往是创建和存放重要数据的场所，绝大部分攻击事件都是从终端发起的，仅仅靠第一种技术进行“防、堵、卡”解决不了问题。TCPA提出“Trusted Computing”的主要目的之一就是为了解决“终端可信”，从TCPA公布的规范来看，“Trusted Computing”并不是什么新技术、新思想，只是对TCB(NTCB)进行了扩展，将密码技术融入TCB(NTCB)中，其实质是第二种技术的扩展和延伸。

2 可信计算的概念

在计算机应用环境中，对“可信”有多种解释，文献[23,40]将“可信”解释为“一个可信的计算机系统所提供的服务可以认证其为可依赖的”；文献[41]将“可信”解释为“如果一个系统或组件的失效会导致安全政策的失败，则这个系统或组件是可信的”；文献[42]将“可信”解释为“如果一个系统按照预期的设计和政策运行，这个系统是可信的”；文献[43]将“可信”解释为“当第二个实体按着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”；文献[44]则将“可信”解释为“可信性是考察行为预期被的满足，这种预期性满足是在多主体多行为范畴内，实现对行为性质、行为输入输出、行为过程、行为属性等方面符合必须遵守的要求、约定、规定、规则、法律的满足性认识与评价”。本文分析了各种“可信”的定义，结合信息安全的现状，采用ISO/IEC15408标准[45]中对“可信”进行了定义：

定义 1 一个可信实体(包括组件、系统或过程)的行为在任意操作条件下是可预测的，并能很好地抵抗应用程序、病毒以及一定的物理干扰造成的破坏。

值得注意的是，可信计算主要着力于解决计算世界当前所面临的普遍的安全威胁和不可信危机，在定义“可信计算”这个概念时，应该注意以下情况：

(1)“可信计算”包含TCG的内容，但不等于TCG。依据TCG的TPM1.1、TPM1.2及相关终端的规范，并不能保证终端的可信。因为依据这些规范，只能达到以下目的：一是密钥和重要数据的安全存放与使用；二是终端运行环境的完整性度量；三是确定终端的身份。但TCG并不能保证终端的内容和行为的可信。另外，“可信计算”也不等于NGSCB。(2)“可信计算”包含终端但不只针对终端，尽管可信计算广受关注源

于终端可信。应该把“可信计算”放到“传统的网络安全技术不能解决当前复杂的网络安全问题”这一大背景下，不仅要包含传统的网络安全技术，而且要能够体现当前的信息安全，特别是网络安全的发展现状和进展。(3)“可信计算”应体现与“可信系统与网络(容错计算)”这个领域的交叉与融合。这种交叉与融合在文献[46-47]中均有论述。(4)“可信计算”应体现信息安全从数据安全时代、网络安全时代到交易安全时代的发展趋势。(5)“可信计算”不是一套规范，也不是一个具体的安全产品或一套针对性的安全解决体系，而是一个有机的信息安全方案，特别是网络安全全方位架构体系化解决方案，是一个保障体系。

为了便于叙述，本文定义“网络元素”的概念。

定义 2　网络元素是指在网络环境中，具有一定功能的系统或实体。

从定义2可以看出，网络元素是广泛的概念。在一个在网络中，各种物理设备，小到二极管，大到计算机，以及各种通讯设备都是网络元素；各种软件系统，如驱动程序、操作系统、数据库系统、应用软件等也都是网络元素。

定义 3　可信计算是研究“网络中网络元素的行为和行为结果，网络元素之间的行为和行为结果总是预期和可控的”的机制、策略、支撑技术、管理等评测方法的总称。

定义3所表述的可信计算，是一个保障体系，既涵盖了传统网络安全的内容，又突出了当前网络安全的新需求；既包含了TCG的终端可信，又体现与可信系统和网络(容错计算)的交叉与融合，较好地满足了当前对可信计算概念的要求。依据定义3，本文可以得出：(1) 可信计算的研究对象是网络元素及其行为以及网络元素之间的行为；(2) 可信计算的目标是网络可信。

3　可信计算的体系结构

根据本文对“可信计算”的定义和网络体系结构，结合当前对“可信计算”的研究现状，提出了如图1所示的可信计算体系结构，该体系结构包括6大部分。

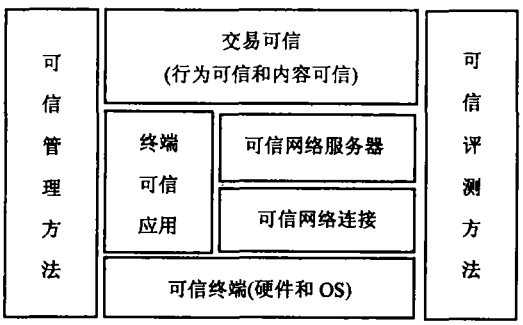

图1　可信计算的体系结构

(1) 可信终端：可信终端是可信计算的一个分支，在整个可信计算体系结构中，处于基础性地位，包括可信硬件和可信OS。(2) 终端可信应用：终端可信应用是指建立在可信终端上的应用，包括应用可信机制、可信应用和操作系统的交互。(3) 可信网络连接：可信网络连接是指网络连接可信，包括可信传输和可信接入。(4) 可信网络服务器：可信网络服务器是指网络中提供服务的服务器是可信的，与可信终端相对应。由于服务器与客户端的地位和作用不同，可信网络服务器应该具有更丰富的内涵。(5) 可信交易：交易是指基于网络的分布式应用；可信交易则是指基于网络的分布式应用是可信的，可信交易的目标是为交易过程提供主体可信性(Subject Trust)、客体可信性(Object Trust)、内容可信性(Contents Trust)和行为可信性(Behavior Trust)的证明，在网络体系和可信计算体系中的抽象层次是最高的。(6) 可信评测方法和管理方法：可信评测方法是对可信计算的评估方法，包括可信等级、评估策略等；可信管理方法是指对所有计算机网络应用体系中各个方面的可信技术和产品进行统一的管理和协调，进而从整体上提高整个计算机网络的可信等级的能力。

当前，人们从多角度、多层次对可信计算进行广泛研究。不同的学者都在强调自己所理解的“可信计算”，并展示自己对“可信计算”的研究成果。这使得“可信计算”的研究虽然“百花齐放”，但呈现一定的盲目性。本文提出可信计算的体系结构，把当前对“可信计算”的绝大部分研究都映射到图1所示的体系结构中。

4　可信计算研究现状

4.1　可信终端

当前，可信终端是“可信计算”中最引人关注的热点之一。国内外产业界包括TCG、Microsoft、IBM、Intel、武汉瑞达、联想等，对可信终端的推动不遗余力。尽管各厂商对“可信计算”的理解不尽相同，但主要思路是在PC机硬件平台上引入安全芯片架构，通过安全芯片提供的安全特性来提高终端系统的安全性，其结构如图2所示。

图2中，可信终端包括含可信硬件的底层硬件和含可信内核的操作系统。可信硬件的主要作用是提供密码保护和安全存储；含可信内核的操作系统的主要作用是提供双重执行环境。在产业界，不同的企业关注点不同。TCG关注可信硬件规范，提出了TPM(Trusted Platform Module)、CRTM(Core Root Trust Module)等各种终端规范[4-5]；Microsoft关注整个终端，提出了终端体系结构NGSCB[48-50]，包括底层安全硬件-安全支持部件(Security Support Component，SSC)、双重执行环境、Nexus可信内核、NCA；Intel提出了新一代PC可信硬件平台解决方案(LaGrande Technology，LT)[51]技术，即LT = CPU + TPM + Chipset + Protected I/O，考虑到兼容性，LT技术还在硬件技术上引入了标准环境和保护环境，并使两种环境可以并存。另外，IBM有自己的可信硬件ESS[52]和可信内核PERSEUS[53]；瑞达有SQY14嵌入密码型计算机[54]；联想则有可信芯片“恒智”[55]。为了促进可信终端的产业化，避免垄断和无序竞争，产业界面临的问题是可信硬件规范和协议的标准化问题。

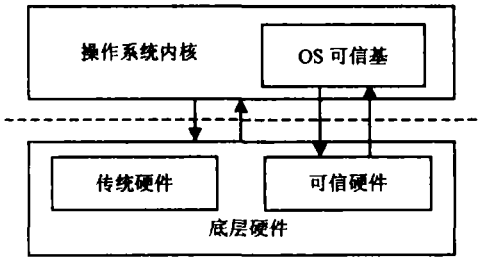

图2 可信终端的基本结构

与产业界的研究相比，学术界更注重可信终端是如何“可信”的，包括“隐私问题”、“证明问题”、“潜在的行为控制问题”，以及“终端行为可信问题”。

“隐私问题”是一个最为敏感的问题，因为可信终端中必须包含用户的身份信息，也就是说，在网络上发生的任何访问动作都能准确定位动作发起者的身份，从而存在暴露用户隐私的巨大隐患。例如对于TCG和NGSCB，虽然它们可以维护数据的机密性，保护了用户的秘密，但却暴露了用户隐私。因为认证需要一个密钥，而所有密钥的根密钥在芯片制备时被永久性植入硬件中，并委托第三方进行认证管理。文献[13-15]分别对隐私问题进行了讨论。目前，还没有好的办法解决隐私问题，因为隐私和可信本来就是一对矛盾。

“证明问题”是一个最为重要的问题，因为终端可信基于证明。可信计算的技术基础是公开的密码技术，为了实现可信计算的证明功能，可信计算技术使用了多种数字证书。例如在TCG的TPM中，包括背书证书(Endorsement Certificate)、符合性证书(Conformance Certificate)、平台证书(Platform Certificate)、验证数字证书(Validation Certificate)和身份证书(Identity Certificate)。引人注目的问题包括由谁签发这些证书、证书的有效期怎样确定、不同机构颁发的证书之间如何交叉认证等。对于这些问题，在证书规模较小的情况下，用PKI容易解决，但是规模一旦增加，PIK就解决不了。大规模证书撤消列表(CRL)的维护是一个最为棘手的问题，文献[56-57]提出了CRL的分段-过量发布模型、增量-过量发布模型，但这些模型缺少实践验证，效果如何还很难下结论。另外，在TCG的TPM中，出于隐私考虑，TPM证言身份证书有效期一般很短，只在一个会话或交易过程中有效，TMP每进行一次会话或交易，需要实时申请证言身份证书，隐私CA的负载很大。为了解决这个问题，TCG提出了直接匿名证言方案(Direct Anonymity Attestation，DAA)，该方案基于零知识证明和群签名技术[58]，较好地解决了隐私CA的负载问题。但是群签名的安全性差、效率低[59]，使DDA的使用存在巨大安全隐患。因此，采用PKI技术不能很好地解决可信计算中的终端身份证明问题。文献[60]提出了基于加密的身份验证(Identity Based Encryption，IBE)算法的认证系统，取消了第三方证明的CA机构。但是，因为需保留大量用户参数，因此仍需参数库的支持。系统靠数据库在线运行，运行效率不会高，处理能量也不会大。文献[61]提出了基于组合公开密钥(Combined Public Key，CPK)算法实现的认证系统。CPK算法也是基于标识的公钥算法，但它不需要第三方证明，因为只需保留少量的公用参数而不需要保留大量用户数据，所以不需要数据库的支持，处理能量和运行效率都很高，因而扩展了其应用范围。

“潜在的行为控制问题”涉及到可信终端的推广，推广问题不解决，可信终端的市场前景很难预料。因此，解决潜在的行为控制问题是一个紧迫的任务。目前，可信终端信任的基础是平台，而非用户自身。例如NGSCB系统中，用户被迫安装被签名的硬件和软件(如NGSCB芯片、OS等)，信任的依据就是这些被签名的硬软件。根据信任关系成立与否，系统实施对行为的控制，也就是可能剥夺用户(即便是计算机系统的所有者)对系统行为的完全控制能力。如只要外部提供者对用户的计算机系统不信任或平台本身认为已存在的实体不可信，他们就能使计算机的拥有者都无法打开其磁盘上的文件，甚至某些设备拒绝启动，或某

些程序拒绝执行。因此，这一机制使得用户存在被控制的可能，内容和程序的限制使用、锁定用户等将变得容易实现，数字权限管理(Digital Rights Manage，DRM)就是一个很好的证明。对于这个问题的解决，除了用户和内容提供商之间的利益折中以外，目前，还没有找到更好的办法。

“终端行为可信问题”是产业界和学术界争论的焦点。产业界认为，只要终端的环境是可信的，密钥和重要数据能安全存放和使用，终端平台身份是可以证明的，那么该终端就是可信的。而学术界认为，产业界所说的可信终端根本就不能使终端完全可信，因为按照“可信”的定义，即使按照TCG对“可信”的定义，也无法保证终端的行为是可以预期和可控制的，也无法保证终端处理的内容是可信的。学术界认为产业界提出的可信终端是概念炒作，商业气味比较浓。完全的可信应该包括终端行为和内容的控制和监管。文献[44]和[62]提出了以代理技术实现终端行为的控制和监管。

4.2 终端可信应用

目前，可信终端并不普及，终端可信应用还很少。但是，可以归纳出终端可信应用需要面对的问题：(1) 如何结合具体的应用环境来利用可信终端的功能；(2) 如何定义终端的可信应用。

对于第一个问题，TCG及Microsoft的NGSCB采用如图3所示的架构，通过代理技术，使得终端的可信应用可以合理地利用可信终端的功能，运行于平台上的双重环境。目前，这是一个可行的办法。存在的困难是如何将OS可信基和代理之间的接口标准化，促进终端可信应用的普及和代理技术如何实现。因为在终端应用中嵌入代理，会增加开发负担，影响终端应用的性能。目前，人们趋向于采用“组件”技术来实现代理，一方面是因为“可信组件”的研究相对比较深入；另一方面是采用“组件”技术可以减少开发负担。

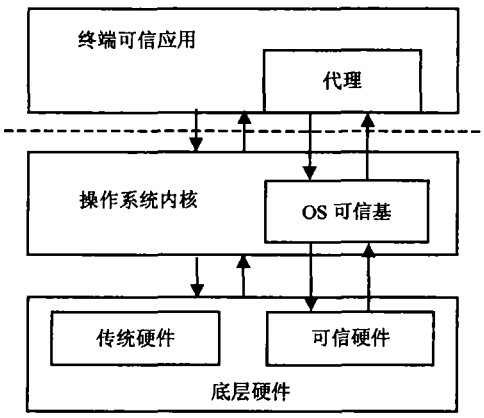

图3　终端可信应用与可信终端的交互

对于第二个问题，通常认为终端可信应用的含义包括两个方面的内容：(1) 从应用的开发过程来衡量应用系统的可信度，并利用CC标准对应用系统进行评估；(2) 该应用在终端上的行为是可预期和可控制的，它的运行不能长期占用和破坏终端的相关资源，但除了传统的身份认证、访问控制和授权以外，目前还没有大的进展。

4.3 可信网络连接

网络中的实体，它们之间的连接不仅仅需要物理设备，还需要传输，因此，可信网络连接应该包括物理设备可信、传输可信和可信接入3个方面。对于物理设备可信，包括两层意思：(1) 物理设备本身，即物理设备本身是否可靠，是否可以采用容错计算技术；(2) 设备的位置安全、限制物理访问、物理环境安全和地域因素等，可以通过可信管理方法解决。所以，可信网络连接包括传输可信问题和可信接入问题。目前，解决可信传输问题的办法是采用可信交换技术，对网络协议进行改进；而解决可信接入问题的方法是对需要接入网络的终端进行检查和控制，确保终端的环境符合一定的要求，访问权限受到控制和监督。

4.3.1 可信传输

可信传输是指为网络实体间在网络交换过程中的发信、转发、接受等提供可信证据，就像现实社会中的邮件，每经一个邮局就要加盖一次印章一样，在每一次转报过程中都要提供经手的证明，如图4所示。

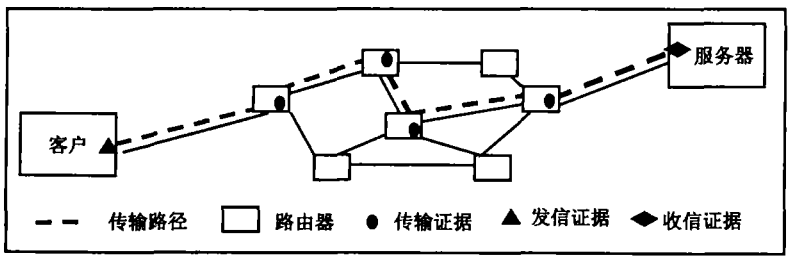

图4　可信传输

但是，目前的网络协议，对如何保证安全传输的问题考虑得不够，更谈不上可信传输了。如作为Internet灵魂协议的TCP/IP，存在着很大的安全隐患，TCP扫描攻击、协议栈指纹鉴别、IP欺骗、DNS欺骗、DoS等，都是利用了TCP/IP的缺陷。如何解决可信传输，目前较好的解决办法是修改网络协议。因此，在可信交换方面最有可能取得进展的技术包括MPLS、ATM和IPv6[63]。

MPLS属于第三层交换技术，引入了基于标记的机制，把选路和转发分开。可信连接由活性标签(Active Label)技术或标签化交换(Labeled Switching)技术规定一个分组通过网络的路径。标签可以在超大规模的网络世界中起“定位”作用，为建立可信传输提供可信证据。

ATM即异步传输模式，曾经被认为是最有希望取代IP的网络技术，尽管到现在还没有流行起来，但应该看到ATM技术本身是先进的。ATM同时支持永久虚电路和交换虚电路。如果采用永久虚电路进行传输，由于传输信道一直存在并且可以任意使用，就像租用的线路一样，因此可以保证可信传输。确保可信传输的方法是，当建立虚电路时，SETUP消息沿着网络从源端走向目的端，路由选择算法决定了消息要走的虚通路(Virtual Path)路径，从而决定了虚电路(Virtual Channel)的路径，可把虚通路的标识和单个信元选择的虚电路标识作为可信证据。

与互联网发展进程中涌现出的其他技术相比，IPv6遇到的争议是最少的，几乎无限的地址容量IPv6最终取代IPv4根本的理由。Ipv6与IPv4相比，除了地址容量的扩充、头部格式的简化、对可选项或扩展项的改进等，还增加了数据流标签能力，以及认证和保密能力，为解决可信传输提供了技术支持。

值得注意的是，MPLS、ATM、IPv6等最初并不是为解决可信传输而提出的，因此，尽管这些技术具有解决可信传输需要的条件，但在网络交换过程中为发信、转发、接受等提供可信证据方面的工作几乎还没有开展，仍然有大量的工作要做。

4.3.2 可信接入

可信接入即网络的准入制度，符合要求的终端才被允许接入网络，并对终端的访问进行授权和控制。传统的网络准入技术包括身份认证、访问控制和授权，但缺少对终端环境的完整性检查，再加上身份认证(如用户名、密码等)的易攻击性，使得传统的网络准入存在较大的安全隐患，也是网络不可信的主要原因之一。其解决的代表性方法有：(1) TGG的可信网络连接(Trusted Network Connection，TNC)[63]；(2) Cisco自动防御网络(Self-Defending Network，SDN)[64]的“网络准入控制(Network Admission Control，NAC)”；(3) “可信认证网关”。

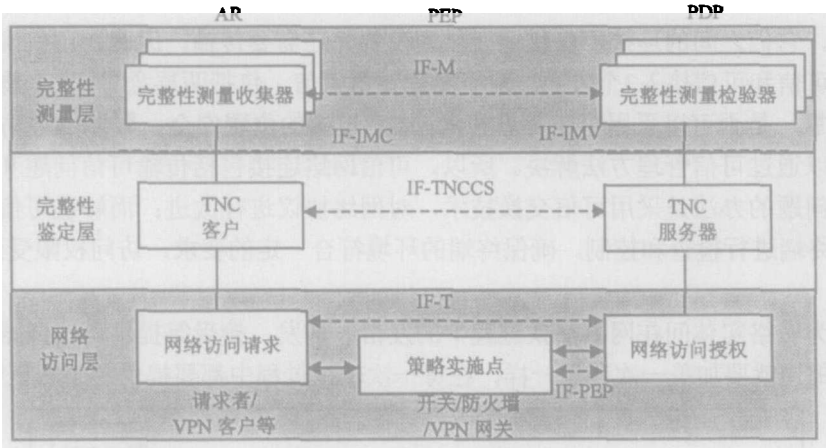

图5 TNC层次图

TCG于2005年4月公布了可信网络连接标准(TNC)[65]架构的详细资料，并提供了实现产品开发的前两个界面，如图5所示。TNC是基于完整性和认证性双重概念开发的。“完整性”是指某端点配置的预期状态，由IT策略所定义，例如系统可以被检查是否遵守预先设定的策略，并且不参与异常或恶意的行为。“认证性”保证系统通过认证只能被授权用户所使用。带有TPM的系统运行时，能够激活TNC以提供一个可信赖的引导机制，这种机制在阻止木马程序时，察觉秘密感染及其他相似攻击的能力是独一无二的。带有与不

带有TPM的系统的混合体也能使用TNC的产品和服务，包括VPN、远程拨号连接、无线网络、802.1x结构和LAN环境在内的多种网络拓扑技术都为TNC架构所支持。TNC架构提供了在不同网络环境中采集和交换端点整合数据的通用框架，基于此架构的产品将使用一系列由客户所在组织的IT部门制定的策略和预定的平台配置，对尝试连接网络的客户进行评估。未满足预定的类似补丁级别、杀毒软件或者操作系统配置等策略的客户，都将被隔离起来以备补救。

网络准入控制(Network Admission Control)是Cisco自防御网络计划的重要组成部分，其核心思想是控制访问权限，有效阻止不符合安全条件的设备及访问进入网络，并将它们置于某个隔离区域之外，或者仅获得对计算资源的有限访问权限，如图6所示。Cisco Security Agent采用基于行为的评估标准来识别和保护服务器及终端计算机，而不仅仅依赖签名匹配来分析识别，成功解决了未知病毒带来的安全风险。Cisco Security Agent整合和扩展了多项终端安全功能，如阻止主机入侵、预防可疑代码、保护操作系统完整性、加固日志等，并把这些功能整合到一个产品内，提供了最大能力的保护。

实现网络准入，基于TCG的可信终端技术的可信认证网关(包括认证服务器和完整性验证服务器)在当前是不可或缺的。认证服务器通过对终端的证言身份证书(AIC)，对终端进行身份认证，确定终端是否包含TPM；完整性服务器检查可信终端的软硬件配置是否满足受保护网络的要求，如果发现客户端具有正确的配置(包括硬件、BIOS、操作系统、补丁和防毒程序等)，就批准客户端接入网络，如图7所示。

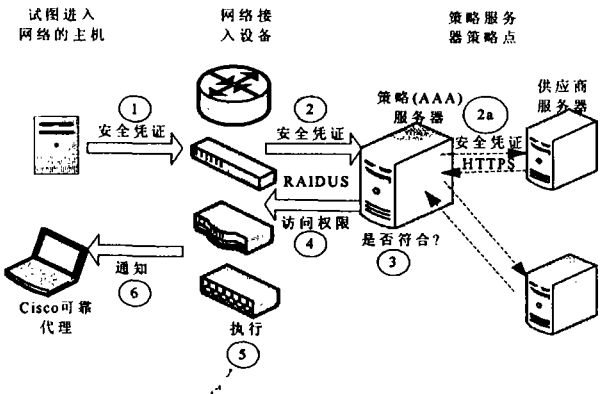

图6　Cisco网络准入控制的原理

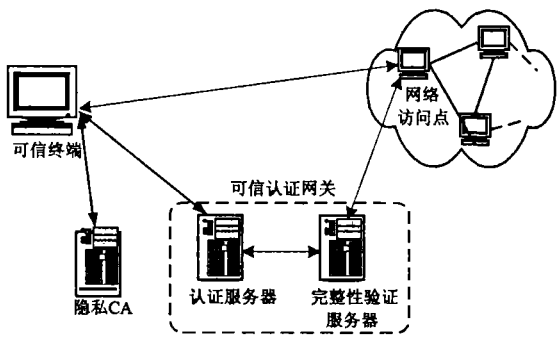

图7　可信认证网关的工作原理

对于上述3种可信接入技术，TNC和可信认证网关均基于TCG的TPM，大量的接口需要定义和标准化，如IF-IMC、IF-IMV等；实体之间的通信需要新的协议，如可信终端与隐私CA、可信终端与可信认证网关等，如图7所示，由于实现起来复杂，离实际使用还有一定的距离。而网络准入控制是Cisco自动防御网络的组成部分，只有使用了Cisco网络接入设备并具有策略服务器的网络才具有使用该技术的条件，因而使用也受到限制。

4.4　可信网络服务器

网络服务器是网络的一个重要组成部分，因此，可信服务器也是可信计算研究的重要问题之一。从传统的网络安全保护手段来看，尽管人们把大量的注意力放在对服务器的保护上，通过安全应用软件如防火墙、入侵检测、防病毒软件等的堆砌来解决服务器的安全可信，但仍然没有取得较好的效果。

对于“服务器可信”，目前有3种观点。高可信计算联盟认为，通过容错、容灾等技术使服务器物理设备可靠和高性能，可满足各种服务需要，因而可信；而TCG认为，服务器可信与终端可信的内涵基本相同，即只要服务器的环境是可信的，密钥和重要数据能安全存放和使用，服务器平台身份是可以证明的，那么该服务器就是可信的。TCG提出了一种带有安全芯片的服务器规范，能更好地保护数据以及交易过程，这一“可信服务器”的蓝本核心仍是TPM，文献[65]公布了“可信服务器”的规范。还有一种观点认为可信网络服务器就是“基于安全操作系统的安全服务器”，采用了操作系统安全加固技术(ROST)。ROST是一项利用安全内核提升操作系统安全等级的技术，在操作系统的核心层重构操作系统的权限访问模型，实现真正的强访问控制，使操作系统达到第三等级，即B1级的安全技术要求。安全服务器需要具备4项安全指标：(1) 安全的物理设备，如控制硬件的拔插、硬件各零件状态的管理检测等；(2) 安全的操作系统，如可以理

解为ROST+普通的操作系统；(3) 安全的应用系统，即在ROST支持下的应用系统；(4) 专业的管理系统，即安全服务器=安全操作系统+安全应用系统+普通服务器。所以ROST的核心意义在于服务器操作系统的可信改造。

总之，当前对“可信服务器”的研究仍然没有摆脱传统的“安全服务器”的思路，对服务器的研究仍然停留在低层次的“可信”上。在服务器中加入TPM会遇到可信终端同样的问题。对“什么样的支撑技术才能保证服务器提供的服务是可预期和可控的，才能保证服务器对共享资源的可信保护”；“如何才能控制服务器的行为”；“怎样评估服务器提供的服务内容可信”等问题的研究还有待深入。

4.5 交易可信

“交易可信”即基于网络的分布式可信应用。与终端可信应用不同，“交易可信”是电子商务和电子政务推广普及的基础和关键，没有“交易可信”，就没有真正意义上的基于Internet的电子商务和电子政务。

“交易可信”是可信计算要考虑的主要内容之一，是可信计算的最高表现形式。此前论述的可信终端、可信网络连接、可信服务器、终端可信应用等都只是可信交易的基础。有学者认为，要使交易可信，就必须在网络与系统上针对业务与技术的行为与行为结果，提供对行为控制、行为监管、行为认证、行为管理和行为对抗的充分能力，并建立相应的体系，以维护网络的可信。在网络中，人们的行为是通过软件的行为来实现的，大量的黑客攻击事件和网络犯罪都有其行为特征，建立自由、平等、方便、安全的网络虚拟世界秩序，光靠研究技术模式是不够的，还必须加深对系统使用者操作行为的研究。

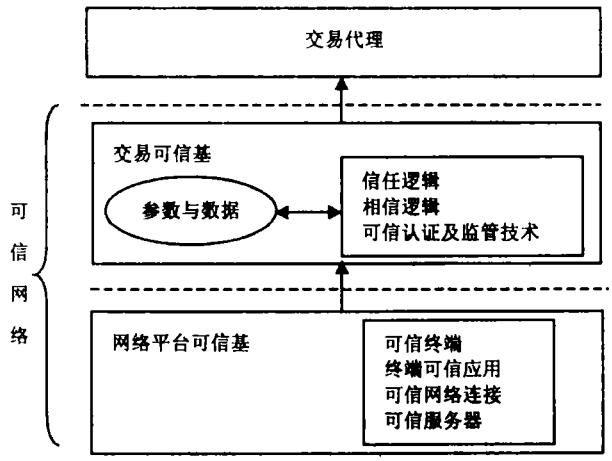

图8 交易可信基

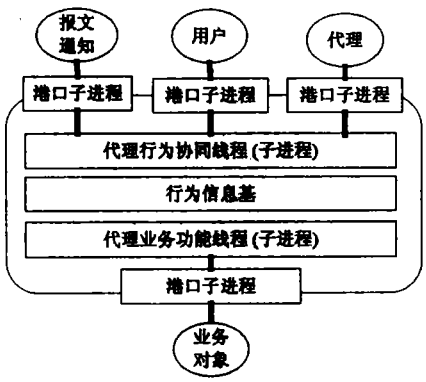

图9 代理技术内部结构图

文献[66]认为，可信交易的目标是为交易过程提供主体可信性(Subject Trust)、客体可信性(Object Trust)、内容可信性(Contents trust)和行为可信性(Behavior Trust)的证明。“主体可信性”通过信任逻辑(Trust Logic)来证明；“客体可信性”通过“相信逻辑”(Belief Logic)来证明；“行为可信性”通过行为可信认证和监管技术来证明。可信交易中，内容和数据是两个不同的概念，内容一般表现为活性客体，即以数据形式存在，但在一定场合下会变成主体。交易可信的体系结构如图8所示。从图8可以看出，交易可信需要代理技术和行为可信认证技术两个关键技术的支撑。

4.5.1 代理技术

可以预见，人类未来在网络中的许多活动与行为将由网络的“可信的虚拟代理主体”实现。现实中的“张三”与网络世界中的“虚拟张三”是一对可信的对应关系.现实中的“张三”将通过“虚拟张三”办很多事情，而这种服务模式要通过代理技术来实现。目前，代理技术已经用于信息安全技术。可信计算平台中的测量、可信连接中的活性标签、可信交易中的行为认证和行为监管等，都可以通过代理技术来实现。代理技术的一般结构如图9所示[44, 63]。

使用代理技术实现可信交易中的行为控制和监管是解决交易可信的有效方法。但在可信计算中使用代理技术，还存在以下问题：

1) 代理，特别是移动代理只有自身可信了，人们才有可能去相信它对主机的行为监控、内容处理可信。这和TCB和NTCB不同，TCB和NTCB得到信任，是因为它们受OS和网络平台的保护，并且满足要求：(1) 具

有自我保护能力; (2) 总是处于活跃状态; (3) 设计得足够小，有利于分析和测试，从而证明它们的实现是正确的。2) 如何对代理自身的行为进行监控，防止代理自身的开域授权。3) 代理需要运行环境，如何保证运行环境的安全和可信。4) 是否需要新的协议实现代理管理平台和代理之间的可信通信，如果需要，在协议和代理中如何留下可信证据。5) 代理和主机之间如何实现行为控制和监管，如何保留控制和监管的可信证据。

以上这些问题不解决，将严重影响可信交易的实现和实现质量。加强代理技术的研究，特别是代理问题本身的研究，是研究可信交易的一个相当紧迫的课题。

4.5.2 行为可信认证技术

行为可信认证是信任理论的基础，也是第三代安全理论的基础。一次行动(Action)可以得到“安全或者不安全”的结论，但却得不到“信任或者不信任”的结论。信任只有通过经常的行动才能体现。因此安全是行动(Action)的结果，而信任则是行为(Behavior)的结果。无论是TPM、可信连接标签、代理活动，还是交易活动都需要认证技术。在网络世界认证系统中，一般都以逻辑参数作为鉴别的主要依据。

目前，存在着3种认证系统: (1) 基于PKI(Public Key Infrastracture)技术实现的认证系统; (2) 基于IBE(Identity Based Encryption)算法实现的认证系统; (3) 基于CPK(Combined Public Key)算法实现的认证系统。表1是PKI、IBE和CPK3种算法的主要功能比较。

表1　PKI、IBE和CPK3种算法的主要功能比较[63]

算法	发布时间/年	层次化CA	数据库	进程鉴别	处理能量
PKI	1996	√	√	×	小
IBE	2001	×	√	×	小
CPK	2004	×	×	√	大

值得注意的是，目前，PKI得到业内巨头的大力支持，并经过了大量的实践检验，其应用在国外已经普及，在证书规模不太大的情况下运转良好。而IBE和CPK是最近才被提出的认证算法，尽管其算法的正确性也得到了理论证明，但是还存在以下问题: (1) IBE和CPK没有经过大量的实践检验; (2) IBE和CPK系统认证的实际效率如何还需要进一步证明; (3) IBE和CPK系统如何与TCB与NTCB进行认证信息交互。

总之，行为可信认证是可信计算的基础，良好的认证系统是可信计算得以实现的前提和支撑技术。尽管理论上提出了好的算法，但实际效果如何，以及如何得到产业界的支持并成为可信计算的认证系统，仍然需要做大量的工作。

4.6 可信评测方法和管理方法

对基于可信计算的产品的评价应该客观、公正，但评价本身属于主观行为，有两个问题需要讨论，一是评价标准; 二是如何为“可信”分等级。

目前，TCG采用的是ISO/IEC 15408(CC)。CC定义了作为评估信息技术产品和系统安全性的基础准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为规范产品和系统安全行为的功能要求，以及正确有效地实施功能要求的保证要求。功能要求和保证要求又以“类-子类-组件”的结构表述。组件作为安全功能的最小构件块，可以用于“保护轮廓”、“安全目标”和“包”的构建。另外，功能组件可以实现CC与传统安全机制和服务的连接，以及解决CC与已有准则如TCSEC、ITSEC的协调关系。对于可信计算，面对的问题是，是否可以用CC作为可信评测标准; 需要做那些修改，以及评测方法是否不同。

信任是有程度之别的，如何为可信分级呢? 如果用CC作为评测标准来评测可信产品，给出的评价结果是定性的，常常只是一个断定产品“可信”或“不可信”的评价结论。这种方法只能在通过评价的产品和未通过评价的产品之间划一个界限，但无论是对已通过评价的产品进行比较，还是对未通过评价的产品进行比较，都无能为力。虽然可以将CC中的保障级别作为评测产品是否可信的依据，但保障级别和可信级别终究是不同的，因此评价可信级别不能完全依据保障级别。文献[67]利用主观逻辑的基本精神[68-69]，给出了CC标准框架下的安全确信度的一种定量描述思想，可以作为可信级别分级评测的一种新手段。

另外，可信系统和可信网络需要科学、可信的管理方法，需要对所有计算机网络应用体系中各个方面的可信技术和产品进行统一的管理和协调，进而从整体上提高整个计算机网络的可信等级的能力。通常，建立一个可信管理体系包括多个方面的建设，全球网络社会管理规范和共同标准、技术上实现的计算机可信管理系统、网络质信的识别和评价系统、电子证据和相关法律、为系统定制的可信管理方针及相应的可信管理制度和人员等。简言之，可信管理包括管理制度和管理技术。在管理制度方面，面对的问题是是否可以用ISO17799[70]作为可信管理的标准，如果能，需要作哪些修改。在管理技术方面，传统的网络管理系统大多都源自网络管理平台的模型，以管理中心和各类Agent作为实现管理的总体框架，以SNMP作为管理协议。目前，新的网络管理趋势是向分布式、智能化和综合化方向发展，如基于Web的管理、基于CORBA的管理、基于JAVA技术的管理和面向智能Agent的开放式管理等[48]。但需面对的问题是，可信管理系统是否需要这些新技术，以及如何将这些新技术应用到可信管理系统的开发中。

总之，在可信计算的体系结构中，对可信评测方法和管理方法的研究是相对薄弱的。由于可信计算与网络安全的紧密关系，多数人包括TCG仍沿用网络安全的评测标准和管理方法，对可信评测和管理的重要性认识得并不充分。

5 总结与展望

随着电子商务和电子政务的进一步发展，对网络环境提出了更高的安全要求，可信计算成为有效解决安全问题的方案。目前，不管是学术界还是产业界，对可信计算的认识还不统一。就可信计算核心支撑技术的研究而言，存在很多复杂问题，如终端和服务端行为和内容的可信问题、终端控制权问题、可信传输的证据问题、代理可信问题、可信评测与管理问题等，有待学术界和产业界研究解决。

参 考 文 献

[1] Mundie C. Remarks on trusted computing forum 2001[EB/OL]. http: // www.microsoft.com/ presspass/exee /eraig, 2006-04-18.
[2] NSF. CISE—trusted computing[EB/OL]. http://www.nsf.gov, 2006-04-21.
[3] TCPA. TPM protection profile v1.9.7, TCPA[EB/OL]. http//www.trustedcomputing.org/home, 2006-04-21.
[4] TCPA. Main specification v1.1b, TCPA[EB/OL]. http//www.trustedcomputing.org/home, 2006-04-25.
[5] TCG Trusted computing group(TCG) main specification version1.1a[EB/OL]. http://www.trustedcomputinggroup.org/ downloads/ tcg_spec_1_1b.zip, 2006-04-30.
[6] TCG TCG PC specific, implementation specification version1.1[]EB/OL]. http://www.trustedcomputinggroup.org/ downloads/ TCG_ PCSpecificSpecification_v1_1.pdf, 2006-04-26.
[7] Department of Computer Science of the Technical University Darmstadt. Trusted systems[EB/OL]. http//www.dvs1 informatik. Tudarmstadt.de/DVIS/research/index.html, 2006-04-28.
[8] 闵应骅. 计算科学的回顾与展望[J]. 自然科学进展, 2000, 10(10): 877-883.
[9] IEEE Computer Society. 50 years of computing, Computer[J]. Innovation Technology Professional, 1996, 29(10):24.
[10] Denning P J, Melcalfe R M. Beyond calculation: The next fifty years of computing[M]. New York: Springer-Verlay New York Inc, 1997.
[11] Department of Computer Science of the Technical University Darmstadt. Trusted systems[EB/OL]. http://www.dvs1 informatik.Tudarmstadt.de/DVIS/research/index.html, 2006-04-29.
[12] 闵应骅. 作为科学的计算科学[M]. 北京: 清华大学出版社, 1994.
[13] Oppliger R, Rytz R. Does trusted computing remedy computer security problems[J]. Security & Privacy Magazine(IEEE), 2005, 3(2):16-19.
[14] Reid J, Nieto J M G, Dawson E, et al. Privacy and trusted computing[C]// Database and Expert Systems Applications: 14th International Workshop, Beijing, 2003.
[15] Felten E W. Understanding trusted computing: Will its benefits outweigh its drawbacks[J]. Security & Privacy Magazine(IEEE), 2003, 1(3): 60-62.
[16] Iliev A, Smith S W. Protecting client privacy with trusted computing at the server[J]. Security & Privacy Magazine(IEEE), 2005, 3(2): 20-28.
[17] Arbaugh B. Improving the TCPA specification[J]. Computer, 2002, 35(8): 77-79.
[18] 侯方勇, 王志英. 可信计算研究[J]. 计算机应用研究, 2004, (12); 1-4.
[19] 刘 鹏, 刘 欣. 可信计算概论[J]. 信息安全与通信保密, 2003, (7): 17-19.
[20] 周明辉, 梅 宏. 可信计算初探[J].计算机科学, 2004, 31(7): 5-8.
[21] Avizienis A. Building dependable systems: How to keep up with complexity[C]// Special Issue FTCS-25, Pasadena, 1995.
[22] 闵应骅. 容错计算二十五年[J]. 计算机学报, 1995, 18(12): 931-943.
[23] TCG The dependable computing[EB/OL]. http://www.dependability.org/,2004.
[24] 闵应骅. 研究动态.[J]计算机研究与发展. 2001, 38(3):380-381.

[25] Laprie J C. Dependable computing: Concepts limits[C]// Special Issue FTCS25, Pasadena, 1995: 42-45.
[26] Andrew S T. Modern operating systems[M]. New York: Prentice Hall Press, 2004.
[27] Willis H W. Report of defense science board task force on computer security[R]. Office of the Director of Defense Research and Engineering, 1970.
[28] DoD 5200.28-STD. Department of defense trusted computer system evaluation criteria[S].1985.
[29] Weissman C. Security controls in the ADEPT-50 time sharing system[C]// AFIPS Fall Joint Computer Conference, New York, 1969.
[30] Butler W L. Dynamic protection structures[C] //AFIPS Fall Joint Computer Conference, Nevada, 1969.
[31] Willis H W. Security controls for computer systems[R]. Defense Science Board Task Force on Computer Security, 1970.
[32] James P A. Computer security technology planning study (Volume II)[R]. Air Force Systems Command, 1972.
[33] CSC-STD-001-83. Department of defense trusted computer system evaluation criteria[S]. 1983.
[34] DoD 5200.29-STD. Department of defense trusted computer system evaluation criteria[S]. 1985.
[35] Marshall D A, Michael V J. Trusted systems concepts[J]. Computer & Security, 1995, (14): 45-56.
[36] Marshall D A, Michael V J. Trusted computing update[J]. Computer & Security, 1995, (14): 57-68.
[37] Marshall D A, Michael V J. New thinking about information technology security[J]. Computer & Security, 1995, (14): 69-81.
[38] National Computer Security Center(NCSC). Trusted network interpretation of the TCSEC NCSC-TG-005[R]. 1987.
[39] 沈昌祥. 构造积极御综合防护体系[J]. 信息安全与保密, 2004, (5): 17-18.
[40] 闵应骅. 可信系统与网络[J]. 计算机工程与科学, 2001, 23(5): 21-28.
[41] Anderson R J. Security engineering: A guide to building dependable distributed systems[M]. New York: Wiley Press, 2001.
[42] Shirley R. Internet security glossary[EB/OL]. http//www.faqs.org/rfcs/rfc2828.html, 2006-04-21.
[43] RFC3280 & RFC2510. Internet X.509 public key infrastructure certificate and certificate revocation list profile. [S]. 1999.
[44] 屈延文. 软件行为学[M]. 北京: 电子工业出版社, 2005.
[45] ISO/IEC 15408-1:1999(E). Common crileria [S]. 1999.
[46] 闵应骅. 可信系统与网络[J]. 计算机工程与科学, 2001, 23(5): 21-28.
[47] 林　闯, 彭雪梅. 可信网络研究[J]. 计算机学报, 2005, 28(25): 751-758.
[48] Carroll. Microsoft "NGSCB": A business overview[EB/OL]. http://wwww.microsoft.com/ presspass/ features/ 2002/ jul02/0724NGSCBwp.asp, 2006-04-28.
[49] Microsoft. Microsoft security model for the next generation secure computing base[EB/OL]. http://www.microsoft.com/resources/ ngscb/documents/ngscb_security_model.doc, 2006-05-02.
[50] Microsoft. Microsoft security model for the next generation secure computing base[EB/OL]. http://www.microsoft.com/resources/ngscb/documents/ngscb_tcb.doc, 2006-05-02.
[51] Intel. Intel LaGrande technology[EB/OL]. http://www.intel.com/technology/security/ LaGrande Technology.
[52] IBM. IBM embedded security subsystem[EB/OL]. http://www.pc.ibm.com/ww/resources/security/securitychip.html, 2006-05-02.
[53] Birgit Pfitzmann. PERSEUS[EB/BL]. http://www.perseusos.org/, 2006-05-02.
[54] 武汉瑞达. 可信计算机系统[EB/OL]. http://www.jetsec.com.cn/product/product.asp, 2006-05-18.
[55] 中国联想. 可信芯片[EB/OL]. http://www.lenovo.com.cn/, 2006-05-18.
[56] 谭　良, 周明天. CRL分段-过量发布断模型[J]. 电子学报, 2005, 133(2): 227-230.
[57] 谭　良, 周明天. CRL增量-过量发布断模型[J]. 计算机科学, 2005, 132(4): 133-136.
[58] Schneier B. Applied cryptography[M]. Beijing: China Machine Press, 1999.
[59] 王贵林, 卿斯汉. 几个门限群签名方案的弱点[J]. 软件学报, 2000, 11(10): 1 326-1 332.
[60] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C] // Lecture Notes in Computer Science, Hongkong, 2001.
[61] Tang Wen, Nan Xiang-Hao, Chen Zhong. Combined public key system[C]// International Conference on Software, Telecommunications and Computer Networks, Beijing, 2004.
[62] TNC. Trusted network connect[EB/OL]. https://www.trustedcomputinggroup.org/groups/network/, 2006-06-05.
[63] Andrew S T. Computer networks [M]. 4 Edition. 北京: 清华大学出版社, 2003.
[64] Cisco. Self-defending network[EB/OL]. http://www.cisco.com/en/US/netsol/ns340/ns394/ns171 /ns413 /networking _solutions_ package.html, 2004-05-10.
[65] TCG TCG generic server specification version 1.0 [EB/OL]. https://www.trustedcomputinggroup.org/groups/server/, 2006-06-06.
[66] 南相浩. 2005信息安全步入"信任"时代[EB\OL]. http://www.venustech.com.cn/tech/aqwz/20050111/2924.htm, 2006-06-08.
[67] 石文昌. 安全操作系统开发方法的研究与实施[D]. 北京: 中国科学院(计算机软件技术研究所), 2001.
[68] Josang A. A logic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311.
[69] Josang A, Peter M M, Cheung E. Web security: The emperors new armour[C]// European Conference on Information Systems (ECIS2001), Bled, 2001.
[70] ISO/IEC. International standard ISO/IEC 17799:2000[EB/OL]. http://www.standardsdirect.org/iso17799.htm, 2006-06-08.

编　辑　熊思亮