普通高等教育“十一五”国家级规划教材

高等学校信息安全系列教材

计算机系统安全(第二版)

曹天杰　张永平　毕方明　编著

高等教育出版社
Higher Education Press

普通高等教育“十一五”国家级规划

高等学校信息安全系列教材

计算机系统安全

（第二版）

曹天杰　张永平　毕方明　编著

高等教育出版社
Higher Education Press

内容提要

本书为普通高等教育“十一五”国家级规划教材，面向应用型本科层次的高校。本书在第一版的基础上进行了细致和严谨的修改，全书分14章，涵盖了密码学、网络安全和系统安全的主要内容。本书从三个层次讲述计算机系统安全的知识：第一层次是理论知识，这一层次主要包括信息安全相关的基本概念、密码学与安全协议的基本知识、网络攻防的原理、访问控制模型等。第二层次是安全应用，包括攻防工具的使用、安全管理与配置。第三层次是安全编程，主要是利用编程技术编写攻防工具，实现信息系统的安全。

本书可作为计算机科学与技术、电子信息科学与技术等专业“计算机系统安全”、“网络安全”课程的教材，也可供从事信息安全管理、开发、服务等工作的人员参考。本书有配套的多媒体课件、网络攻防案例库供读者下载。

图书在版编目(CIP)数据

计算机系统安全/曹天杰，张永平，毕方明编著. —2版.
—北京：高等教育出版社，2007.11
ISBN 978-7-04-022073-5

Ⅰ.计… Ⅱ.① 曹… ② 张… ③ 毕… Ⅲ.电子计算机-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆CIP数据核字（2007）第159431号

策划编辑 武林晓 **责任编辑** 萧 潇 **封面设计** 于文燕 **责任绘图** 朱 静
版式设计 马敬茹 **责任校对** 姜国萍 **责任印制** 朱学忠

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	人民教育出版社印刷厂	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2003年9月第1版 2007年11月第2版
印 张	21	**印 次**	2007年11月第1次印刷
字 数	470 000	**定 价**	28.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 22073-00

第二版前言

本书第一版从2003年出版以来，一直深受广大读者的好评，相继被许多高校选定为教科书和参考书。这次对本书进行了认真和全面的修订，形成第二版，并被列入普通高等教育“十一五”国家级规划教材。

第二版对第一版的内容进行了优化和适当增删，并对一些章节进行了调整。主要修改内容是：第四章密码学基础中的AES叙述更详细，第五章消息认证中删除了MD5的描述，第六章增加了数字证书的使用、权限管理基础设施，第七章重写了基于口令的认证、增加了EKE协议，第八章对访问控制的内容进行了重新组织，第九章防火墙增加了网络地址转换、代理服务器的使用，第十章攻击与应急响应，补充了资料并对内容进行了重新组织，第十二章计算机取证为新增内容。

本书由曹天杰、张永平、毕方明编写，其中第一章至第四章由张永平编写，第九章、第十一章至第十四章由毕方明编写，其余部分由曹天杰编写。本书的出版得到江苏省自然科学基金(BK2007035)和中国矿业大学科技基金的资助。

本书有配套的多媒体课件和网络攻防案例库，读者可在高等理工教学资源网(http://www.hep-st.com.cn)下载。欢迎读者对本书的不足批评指正，编者的电子邮箱是tjcao@cumt.edu.cn。

编者

2007年8月

第一版前言

计算机在政治、军事、金融、商业等部门的应用越来越广泛，社会对计算机网络信息系统的依赖也越来越大，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱，随着全球安全事件的逐年增多，确保网络信息系统的安全已引起世人的关注，信息安全在各国都受到了前所未有的重视。“9·11”之后，美国联邦调查局所属的关键性基础设施保护中心发布了《关于网络空间安全的国家战略》的报告，明确地将信息安全提升到了关系国家安全的战略高度，“信息安全＋国土安全＝国家安全”正逐渐得到社会的认同。

我国正逐步形成一个完善的统一的安全保障体系，成立了国家计算机网络应急处理协调中心（简称 CNCERT，http：//www.cert.org.cn /）、国家计算机病毒应急处理中心（http：//www.antivirus-china.org.cn /）、国家计算机网络入侵防范中心（http：//www.nipc.org.cn /）、信息安全国家重点实验室（http：//www.is.ac.cn /）等一批国家级机构。信息安全、信息对抗、密码学等专业已开始在许多高校及科研院所招生，并开设了“计算机系统安全”、“密码学”等相关课程，但目前我国信息安全人才依然缺乏，内容系统全面反映最新进展的优秀本科信息安全教材还不多见。

根据“计算机系统安全”的教学需要，我们从 2000 年开始编写讲义，在多年讲授该课程的基础上，不断充实改进，完成了本教材。

安全的概念是与时俱进的，历经了可靠性、保密、保护，而发展到今天的信息保障。本书从技术的角度介绍了信息安全保障体系，从管理的角度介绍了风险管理，并进一步强调系统安全是一个动态的整体的安全。

本书内容全面、系统，涉及了计算机系统安全的主要方面，如物理安全、运行安全（风险分析、审计跟踪、备份与恢复、应急）、信息安全（网络安全、访问控制、认证等）。全书分十三章：计算机系统安全概述、计算机系统的物理安全、计算机系统的可靠性、密码学基础、消息认证与数字签名、公开密钥基础设施 PKI、身份认证、访问控制、防火墙、攻击与应急响应、入侵检测、IP 安全、安全套接层（SSL）协议。

本书选材合理，结构紧凑。例如作为信息安全基础的密码学，内容十分丰富，1976 年 W. Diffie 和 M.E.Hellman 发表的《密码学的新方向》，以及 1977 年美国公布实施的数据加密标准 DES，标志着密码学发展的革命。2001 年 11 月美国国家标准技术研究所 NIST 发布的高级数据加密标准 AES 代表着密码学的最新发展。本书以简练的语言涵盖了现代密码学的基本内容，介绍了用于军事、移动通信领域的序列密码，分析了简洁、快速、适于软 /硬件加密并且已经标准化的 DES、AES 等典型分组密码，叙述了适合于数字签名、身份认证、密钥交换等领域的公开密钥

密码，并讨论了应用广泛的 RSA 算法。

本书内容反映了近几年计算机系统安全领域的新发展。如介绍了密码体制的可证明安全、语义安全，介绍了取代 DES 的美国高级数据加密标准 AES、零知识身份证明、基于角色的访问控制 RBAC、代理服务技术、IDS 的标准化、风险管理与应急响应，等等。

本书参考了大量的 RFC 文档(http: //www.ietf.org /rfc.html)、美国国家标准技术研究所出版物(http: //csrc.nist.gov /publications /)，也希望读者在学习的过程中查阅参考。

本书适合计算机科学与技术、信息安全等专业本科使用，可以作为“计算机系统安全”、“计算机网络安全”等相关课程的教材，也可以作为工程技术人员系统地学习信息安全理论的参考书。

编者感谢信息安全国家重点实验室的林东岱研究员、南开大学数学科学学院的胡健伟教授和孙澈教授给予的指导。感谢信息安全国家重点实验室的博士后徐涛、博士后黄寄宏、博士生孙海波、硕士生李绪蜂、硕士生孟江涛、中科院数学与系统科学研究所的硕士生程贯中、北京大学数学学院的硕士生魏晋伟等的热情支持，感谢中国矿业大学计算机学院的夏士雄院长、张虹教授、殷兆麟教授，感谢南京大学计算机科学与技术系的黄皓教授、博士生林果园等在本教材的编写过程中给予的各种不同形式的帮助。

信息安全国家重点实验室的薛锐研究员仔细审阅了本书，提出了许多宝贵的意见和建议，编者在此表示特别的感谢。

编者衷心希望读者对本教材批评指正。

曹天杰

于中国科学院软件所信息安全国家重点实验室

2003 年 6 月

目　录

第一章　计算机系统安全概述

1.1　计算机系统安全的概念

1.1.1　世界范围内日益严重的安全问题

信息技术和信息产业正在改变传统的生产、经营和生活方式，信息已成为社会发展的重要战略资源。社会对网络信息系统的依赖也日益增强，信息网络已经成为社会发展的重要保证。

在计算机应用日益广泛和深入的同时，计算机网络的安全问题也日益复杂和突出。网络的脆弱性和复杂性增加了威胁和攻击的可能性。从以下数据可以看出网络信息安全问题的重要性。

1986 年初在巴基斯坦的巴锡特(Basit)和阿姆杰德(Amjad)两兄弟编写的 Pakistan(即 Brain)病毒在一年内流传到了世界各地。

1988 年 11 月，美国康奈尔大学的学生 Morris 编制的名为蠕虫的计算机病毒通过 Internet 传播，致使网络中约 7 000 台计算机被传染，Internet 不能正常运行，迫使美国国防部立即成立了计算机应急行动小组，以消除此事件造成的影响。Morris 蠕虫造成经济损失约 1 亿美元。这是一次非常典型的计算机病毒入侵计算机网络的事件。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他 80 多个军方网站。

2003 年的蠕虫王、冲击波，2004 年的震荡波，2005 年的极速波等蠕虫爆发，都造成了巨大的经济损失。

现在人们经常听到黑客(hacker)这个词，那么黑客到底是指哪些人呢？黑客在信息安全范畴内是特指对计算机系统的非法侵入者。美国警方把所有“利用”、“借助”、“通过”或“阻挠”计算机系统的犯罪行为都定义为 hacking。中国的一些黑客自称红客(honker)。入侵者(cracker)是指怀着不良的企图，闯入甚至破坏远程计算机系统完整性的人。入侵者利用获得的非法访问权，破坏重要数据，拒绝合法用户服务请求，或为了自己的目的制造麻烦。

1.1.2　计算机系统安全的概念

在 20 世纪 40—50 年代，人们认为安全就是通信保密，采用的保障措施就是加密和基于计

算机规则的访问控制，这个时期被称为“通信保密(COMSEC)”时代，其代表事件是 1949 年 Shannon 发表《保密通信的信息理论》。在 20 世纪 70 年代，人们关心的是计算机系统不被非授权用户使用，这个阶段学术界称之为“计算机安全(INFOSEC)”时代，其代表事件是美国 20 世纪 80 年代初发布橘皮书——可信计算机评估准则(TCSEC)。20 世纪 90 年代，人们关心的是如何防止通过网络对联网计算机进行的攻击，这个阶段学术界称之为“网络安全(NETSEC)”时代，其代表事件是美国 20 世纪 80 年代末出现的 Morris 蠕虫盛行。进入 21 世纪，人们关心的是信息及信息系统的保障，如何建立完整的保障体系，以保障信息及信息系统的正常运行，这个阶段学术界称之为“信息保障(IA)”时代。

从技术角度看，计算机系统安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。首先介绍以下几个概念。

1. 计算机系统安全

计算机系统(Computer System)也称计算机信息系统(Computer Information System)，是由计算机及其相关和配套的设备、设施(含网络)构成的，并按一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。计算机系统安全(Computer System Security)中的“安全”一词是指将服务与资源的脆弱性降到最低限度。脆弱性是指计算机系统的任何弱点。由于信息是重要的战略资源，计算机系统集中管理着国家和企业的政治、军事、金融、商务等重要信息，因此计算机系统成为不法分子的主要攻击目标，计算机系统安全成为世人关注的社会问题。

国际标准化组织(ISO)将“计算机安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”此概念偏重于静态信息保护。也有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

2. 计算机系统安全属性

在美国国家信息基础设施(NII)的文献中，给出了安全的 5 个属性：可用性、可靠性、完整性、保密性和不可抵赖性。这 5 个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。这 5 个属性定义如下。

① 可用性(Availability)：得到授权的实体在需要时可访问资源和服务。可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的和多方面的(语音、数据、文字和图像等)，有时还要求时效性。网络必须随时满足用户通信的要求，攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括有效地避免因各种灾害(战争、地震等)造成的系统失效。

② 可靠性(Reliability)：可靠性是指系统在规定条件下和规定时间内完成规定功能的概率。

可靠性是网络安全最基本的要求之一,网络不可靠,事故不断,也就谈不上网络的安全。目前,对于网络可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备,采取合理的冗余备份措施仍是最基本的可靠性对策,然而,有许多故障和事故则与软件可靠性、人员可靠性和环境可靠性有关。

③ 完整性(Integrity):信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程,并且能够判别出实体或进程是否已被篡改,即信息的内容不能为未授权的第三方修改,信息在存储或传输时不被修改、破坏,不出现信息包的丢失、乱序等。

④ 保密性(Confidentiality):保密性是指确保信息不暴露给未授权的实体或进程,即信息的内容不会被未授权的第三方所知。这里所指的信息不但包括国家秘密,而且包括各种社会团体、企业组织的工作秘密及商业秘密,个人的秘密和个人私密(如浏览习惯、购物习惯)。防止信息失窃和泄露的保障技术称为保密技术。

⑤ 不可抵赖性(Non-Repudiation):也称为不可否认性。不可抵赖性是面向通信双方(人、实体或进程)信息真实、同一的安全要求,包括收、发双方均不可抵赖。不可抵赖性包括两个方面:一是源发证明,它提供给信息接收者以证据,这将使发送者谎称未发送过这些信息或者否认它的企图不能得逞;二是交付证明,它提供给信息发送者以证明,这将使接收者谎称未接收过这些信息或者否认它的企图不能得逞。

除此之外,计算机网络信息系统的其他安全属性还包括:

⑥ 可控性:可控性就是对信息及信息系统实施安全监控。管理机构对危害国家信息的来往、使用加密手段从事的非法通信活动等进行监视、审计,对信息的传播及内容具有控制能力。

⑦ 可审查性:使用审计、监控、防抵赖等安全机制,使得使用者(包括合法用户、攻击者、破坏者、抵赖者)的行为有据可查,并能够对网络出现的安全问题提供调查依据和手段。审计是通过对网络上发生的各种访问情况记录日志,并对日志进行统计分析,是对资源使用情况进行事后分析的有效手段,也是发现和追踪事件的常用措施。审计的主要对象为用户、主机和结点,主要内容为访问的主体、客体、时间和成败情况等。

⑧ 认证:保证信息使用者和信息服务者都是真实声称者,防止冒充和重放的攻击。

⑨ 访问控制:保证信息资源不被非授权地使用。访问控制根据主体和客体之间的访问授权关系,对访问过程做出限制。

3. 计算机系统安全的范畴

安全工作的目的就是在安全法律、法规、政策的支持与指导下,通过采用合适的安全技术与安全管理措施,维护计算机系统安全。我们应当保障计算机及其相关和配套的设备、设施(含网络)的安全,保障运行环境的安全,保障信息的安全,保障计算机功能的正常发挥,以维护计算机信息系统的安全运行。从作用层面来看,人们首先关心的是计算机与网络的设备硬件自身的安全,就是信息系统硬件的稳定性运行状态,因而称为"物理安全";其次关心的是计算机与网络设备运行过程中的系统安全,就是信息系统软件的稳定性运行状态,因而称为"运行安全";当讨论

信息自身的安全问题时，涉及的就是狭义的“信息安全”问题，包括对信息系统中所加工、存储和网络中所传递数据的泄漏、仿冒、篡改以及抵赖过程所涉及的安全问题，也称为“数据安全”。

(1) 物理安全(Physical Security)

保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施、过程。特别是避免由于电磁泄漏产生信息泄露，从而干扰他人或受他人干扰。物理安全包括环境安全、设备安全和媒体安全 3 个方面。

(2) 运行安全(Operation Security)

为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失。运行安全包括风险分析、审计跟踪、备份与恢复和应急 4 个方面。

风险分析是指为了使计算机信息系统能安全地运行，首先要了解影响计算机信息系统安全运行的诸多因素和存在的风险，从而进行风险分析，找出避免这些风险的方法。

审计跟踪是利用计算机信息系统所提供的审计跟踪工具，对计算机信息系统的工作过程进行详尽的跟踪记录，同时保存好审计记录和审计日志，并从中发现和及时解决问题，保证计算机信息系统安全可靠地运行。这就要求系统管理员要认真负责，切实保存、维护和管理审计日志。

应急措施和备份恢复应同时考虑。首先要根据所用信息系统的功能特性和灾难特点制订包括应急反应、备份操作、恢复措施 3 个方面内容的应急计划，一旦发生灾害事件，就可按计划方案最大限度地恢复计算机系统的正常运行。

(3) 信息安全(Information Security)

信息成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式。信息产业成为新的经济增长点。社会的信息化已成为当今世界发展的潮流和核心。信息获取能力和信息的安全保障能力成为综合国力的重要组成部分。信息安全事关国家安全，事关社会稳定。

防止信息财产被故意或偶然地非授权泄露、更改、破坏或使信息被非法的系统辨识、控制，即确保信息的完整性、保密性、可用性和可控性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密和鉴别 7 个方面。

网络信息既有存储在网络结点上的信息资源，即静态信息，又有传播于网络结点间的信息，即动态信息。而这些静态信息和动态信息中，有些是开放的，如广告、公共信息等；有些是保密的，如私人间的通信、政府及军事部门、商业机密等。

前面已经介绍了人们所关注的 3 个层面，即物理安全、运行安全及信息安全。但是，还有两个层面没有给出描述，一个是关于信息内容的安全，一个是关于信息对抗。内容安全更被文化、传媒界人士所关注；而信息对抗则更被电子对抗研究领域的人士所关注。

内容安全的问题已经严重地影响了现实社会，主要表现为有害信息利用互联网所提供的自由流动的环境肆意扩散，其信息内容或者像脚本病毒那样给接收信息的系统带来破坏性的后果，或者像垃圾邮件那样给人们带来烦恼，或者像谣言那样给社会大众带来困惑，从而成为导致社会

不安定的因素。但是,就技术层面而言,信息内容安全技术的表现形式是对信息流动的选择控制能力,换句话说,表现出来的是对数据流动的攻击特性。

信息对抗严格上说是信息谋略范畴的内容,是讨论如何从多个角度或侧面来获得信息并分析信息,或者在信息无法隐藏的前提下,通过增加更多的无用信息来扰乱获取者的视线,以掩藏真实信息所反映的含义。从本质上来看,信息对抗是在信息熵的层面上讨论问题,也就是围绕着信息的利用来进行的。

我国公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门,在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法,由公安部会同有关部门制订。计算机信息系统的使用单位应当建立、健全安全管理制度,负责本单位计算机信息系统的安全保护工作。

1.1.3 国内外计算机系统安全标准

1. 国外计算机系统安全标准

制订计算机系统安全标准的国际性的标准化组织主要有国际标准化组织(ISO)、国际电器技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组(ITU-TS)。

美国国防部的可信计算机系统评价准则(Trusted Computer System Evalution Criteria, TCSEC,又称橘皮书)是计算机系统安全评估的第一个正式标准,具有划时代的意义。该准则于1970年由美国国防科学委员会提出,并于1985年12月由美国国防部公布。TCSEC将安全分为4个方面:安全政策、可说明性、安全保障和文档。该标准将以上4个方面分为7个安全级别,按安全程度从最低到最高依次是D、C1、C2、B1、B2、B3、A1。

① D类:最低保护,无需任何安全措施。属于这个级别的操作系统有:DOS、Windows、Apple的Macintosh System 7.1。

② C1类:自决的安全保护。系统能够把用户和数据隔开,用户可以根据需要采用系统提供的访问控制措施来保护自己的数据,系统中必须有一个防止破坏的区域,其中包含安全功能。用户拥有注册账号和口令,系统通过账号和口令来识别用户是否合法,并决定用户对程序和信息拥有什么样的访问权。

③ C2类:访问控制保护。控制粒度更细,使得允许或拒绝任何用户访问单个文件成为可能。系统必须对所有的注册,文件的打开、建立和删除进行记录。审计跟踪必须追踪到每个用户对每个目标的访问。能够达到C2级的常见操作系统有:UNIX系统、XENIX、Windows NT。

④ B1类:有标签的安全保护。系统中的每个对象都有一个敏感性标签,而每个用户都有一个许可级别,许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签,任何对用户许可级别和成员分类的更改都受到严格控制。较流行的B1级操作系统是OSF/1。

⑤ B2 类:结构化保护。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块;实施最少特权原则。必须对所有目标和实体实施访问控制。政策要由专职人员负责实施,要进行隐蔽信道分析。系统必须维护一个保护域,保护系统的完整性,防止外部干扰。目前,UNIXWare 2.1/ES 是国内独立开发的具有自主知识产权的高安全性 UNIX 系统,其安全等级为 B2 级。

⑥ B3 类:安全域。系统的安全功能足够小,以便于广泛测试。必须满足参考监视器需求以传递所有的主体到客体的访问。要有安全管理员,审计机制扩展到用信号通知安全相关事件,还要有恢复规程,系统高度抗侵扰。

⑦ A1 类:核实保护。最初设计系统就充分考虑安全性问题,有"正式安全策略模型",其中包括由公理组成的数学证明。系统的顶级技术规格必须与模型相对应,系统还包括分发控制和隐蔽信道分析。

1991 年,欧共体发布了信息技术安全评价准则(Information Technology Security Evaluation Criteria,ITSEC)。1993 年,加拿大发布了加拿大可信计算机产品评价准则(CTCPEC),CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年,美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上,发布了美国信息技术安全评价联邦准则 (FC)。ITSEC 与 TCSEC 不同,其观点是应当分别衡量安全的功能和安全的保障,而不应像 TCSEC 那样混合考虑安全的功能和安全的保障。因此,ITSEC 对每个系统赋予两种等级:"F"(Functionality)即安全功能等级,"E"(European Assurance)即安全保障等级。另外,TCSEC 把保密作为安全的重点,而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。CTCPEC 标准将安全需求分为 4 个层次:机密性、完整性、可靠性和可说明性。FC 参照了 CTCPEC 及 TCSEC,在美国的政府、民间和商业领域得到广泛应用。1993 年 6 月,上述国家共同起草了一份通用准则(CC),并将 CC 推广为国际标准。1999 年 10 月 CC v2.1 版发布,并且成为 ISO 标准。CC 结合了 FC 及 ITSEC 的主要特征,它强调将安全的功能与保障分离,并将功能需求分为 9 类 63 族,将保障分为 7 类 29 族。

ISO 在安全体系结构方面制定了国际标准 ISO7498-2:1989《信息处理系统开放系统互连基本参考模型第 2 部分:安全体系结构》。该标准提供了安全服务与有关机制的一般描述,确定在参考模型内部可以提供这些服务与机制的位置。

2. 国内计算机系统安全标准

国内由公安部主持制定、国家技术标准局发布的国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》将信息系统安全分为 5 个等级,分别是:自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等,这些指标涵盖了不同级别的安全要求。我国红旗安全操作系统 RFSOS 2.0 已通过我国公安部计算机信息系统产品质量监督检验中心的认证,达到信息安全第三级的要求。