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3版)

曹天杰　张立江　张爱娟　编著

高等教育出版社
HIGHER EDUCATION PRESS

普通高等教育“十一五”国家级规划教材

高等学校信息安全系列教材

计算机系统安全

Jisuanji Xitong Anquan

（第3版）

曹天杰　张立江　张爱娟　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本版在第2版的基础上，增加了信息安全理论与实践的最新进展，进行了细致和严谨的修改，面向应用型本科层次的高校。全书分为14章，涵盖了密码学、网络安全和系统安全的主要内容。本书从三个层次介绍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的基本概念、密码学与安全协议的基本知识、网络攻防原理、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开发攻防工具、实现安全的信息系统。

本书可作为计算机科学与技术、网络工程、软件工程等专业“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。

图书在版编目(CIP)数据

计算机系统安全/曹天杰，张立江，张爱娟编著.
--3版. --北京:高等教育出版社，2014.1
ISBN 978-7-04-039113-8

Ⅰ.①计… Ⅱ.①曹… ②张… ③张… Ⅲ.①计算机网络-安全技术-高等学校-教材 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2013)第300312号

策划编辑 武林晓　责任编辑 武林晓　封面设计 于文燕　版式设计 杜微言
插图绘制 尹文军　责任校对 刘 莉　责任印制 刘思涵

出版发行 高等教育出版社
社 址 北京市西城区德外大街4号
邮政编码 100120
印 刷 山东省高唐印刷有限责任公司
开 本 850mm×1168mm 1/16
印 张 20
字 数 440千字
购书热线 010-58581118
咨询电话 400-810-0598

网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn

版 次 2003年9月第1版
2014年1月第3版
印 次 2014年1月第1次印刷
定 价 29.80元

物料号 39113-00

第 3 版前言

本书被许多高校选定为教科书和参考书，深受广大师生欢迎。

本书第 1 版自 2003 年出版以来，至 2006 年，共印刷 7 次，累计印数达 35 000 册；第 2 版自 2007 年 12 月出版以来，至 2012 年共印刷 5 次，累计印数达 15 000 册。随着移动互联网、物联网、云计算、电子商务等信息技术的发展，信息安全领域的理论与实践日新月异，网络攻击出现了新的动向。

本版在第 2 版的基础上增加了信息安全理论与实践的最新进展，参考了大量资料，精心选材，进行了细致和严谨的修改，增加的内容主要包括 PPDRR 安全模型、基于图形口令的认证、双因子认证、渗透攻击与渗透测试、0DAY 漏洞、网页挂马、手机病毒、高级持续性威胁、SQL 注入攻击、跨站脚本攻击、信息系统等级保护，并对其他章节进行了全面删改。

本书由曹天杰、张立江、张爱娟编写，研究生曹黎波、柴婷婷、刘文卓参与了部分工作。

本书有配套的多媒体课件供读者下载，读者可在中国高校计算机课程网（http://computer. cncourse. com）下载，也可通过发送电子邮件到 tjcao@ cumt. edu. cn 索取最新的课件、试卷、教学大纲、实验指导书等课程资料。欢迎读者对本书的不足进行指正。

编者

2013 年 7 月

第 2 版前言

本书第 1 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 2 版。

第 2 版对第 1 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，进行了重新组织、增加了新材料，第十二章增加了计算机取证的内容。

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、网络攻防案例库供读者下载，读者可在中国高校计算机课程网（http://computer. cncourse. com）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 1 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”事件之后，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。在当今信息时代，我们面临信息战的威胁。

我国正逐步形成一个完善、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，内容全面、专业、系统、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，在讲授了该课程多年的基础上，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、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。

本书内容反映了近年计算机系统安全领域的新概念、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;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、博士生林果园在本教材的编写过程中给予的各种不同形式的帮助。

最后编者特别感谢高等教育出版社的刘建元编审为本书的出版所付出的辛勤劳动,感谢信息安全国家重点实验室的薛锐研究员审稿中指出的缺点及改进建议。

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 1 章　计算机系统安全概述

1.1　计算机系统的安全问题及基本概念

1.1.1　世界范围内日益严重的信息安全问题

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，与此同时，安全问题也越发突出。

1986 年初，在巴基斯坦的拉合尔（Lahore）、巴锡特（Basit）和阿姆杰德（Amjad）编写的 Pakistan 病毒（即 Brain）在一年内流传到了世界各地。

1988 年 11 月，美国康乃尔大学的学生莫里斯（Morris）编制的名为蠕虫的计算机病毒通过因特网传播，致使网络中约 7 000 台计算机被传染，Internet 不能正常运行，迫使美国政府立即做出反应，国防部成立了计算机应急行动小组。蠕虫病毒当时造成经济损失约 1 亿美元。

之后的互联网安全威胁主要经历了以下 4 个阶段。

① 蠕虫阶段（2001—2004 年）：以蠕虫为代表的“损人不利己”式攻击方式为主。

② 网络犯罪阶段（2004—2007 年）：出现大量趋利性的攻击。

③ 网络窃密阶段（2007—2010 年）：出现大量互联网窃密行为。

④ 新安全阶段（2010 年后）：以针对特定目标与系统的高级持续性威胁（Advanced Persistent Threat，APT）为代表。

1.1.2　计算机系统安全的概念

早在 20 世纪四五十年代，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，其时代标志是 1949 年 Shannon 发表的《保密通信的信息理论》；在 70 年代，人们关心的是计算机系统不被他人非授权使用，学术界称为“计算机安全（INFOSEC）”时代，其时代特色是美国 80 年代初发布的橘皮书——可信计算机评估准则（TCSEC）；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攻击，这时学术界称为“网络安全（NETSEC）”时代，其时代特征是美国 80 年代末出现的“莫里斯”蠕虫事件；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，以便保障

信息及信息系统的正常运行，这时学术界称为“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)也称为计算机信息系统(Computer Information System)，是由计算机及其相关的和配套的设备、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。

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上的和管理上的安全保护，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、机密性和不可抵赖性。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。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，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，从而提高可用性。

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。可靠性是安全最基本的要求之一，系统不可靠，事故不断，也就谈不上安全。目前，对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，有许多故障和事故还与软件可靠性、人员可靠性和环境可靠性有关。

③ 完整性(Integrity)：信息在存储或传输时不被偶然或蓄意地删除、修改、伪造、乱序、重放(重演)、插入等破坏的特性。只有得到允许的人才能修改信息，或者能够判别出信息是否已被篡改。非法写是对完整性的破坏。

④ 机密性(Confidentiality)：机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，个人的隐私(如住所、交际、浏览习惯、购物习惯)。匿名性可以看做用户身份的机密性。非法读是对机密性的破坏。

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,它包括收、发双方均不可抵赖。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信息内容的企图不能得逞;二是交付证明,它提供给信息发送者以证据,这将使接收者谎称未接收过这些信息或者否认信息内容的企图不能得逞。

除此之外,计算机网络信息系统的其他安全属性还包括以下几个。

⑥ 可控性(Controllability):可控性就是对信息及信息系统实施监控。管理机构对危害国家的信息来往、从事的非法活动等进行监视、审计、控制、取证,如对不良信息的传播进行拦截。

⑦ 可审查性(Accountability):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)的行为有证可查,并且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、主机和节点,主要内容为访问的主体、客体、时间和成败情况等。

⑧ 认证(Authentication):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(Access Control):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。

根据具体的应用场景,不同的用户看重系统的不同属性。如用户看重隐私保护,国家机关看重可控性、可审查性。

3. 计算机系统安全的范畴

安全工作的目的就是为了在安全法律、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。应当保障计算机及与其相关的和配套的设备、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(Physical Security)";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(Operation Security)";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(Information Security)"问题,包括对在信息系统中加工和存储的、在网络中传递的数据的泄露、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

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

为了保障系统功能的安全实现,提供一套安全措施(如风险分析、审计跟踪、备份与恢复、应急等)来保护信息处理过程的安全。它侧重于保证系统正常运行,避免由于系统的崩溃和损坏

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、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,找出克服这些风险的方法。

审计跟踪是指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。根据所用信息系统的功能特性和灾难特点制定包括应急反应、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,就可以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

信息已成为社会发展的重要战略资源,信息技术正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地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、加密与鉴别7个方面。

网络信息既有存储于网络节点上的信息资源,即静态信息,又有传播于网络节点间的信息,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、政府及军事部门的机密、商业机密等。

前面已经介绍了人们所关注的3个层面,即物理安全层、运行安全层及数据安全层。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问题;另一个是关于信息对抗的问题。内容安全是文化、宣传界人士所关注的;而信息对抗则是电子对抗研究领域的人士更加关注的。

内容安全的问题已经展现在公众面前,主要表现在有害信息通过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的信息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,从而成为社会不稳定因素。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,讨论的是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,以掩藏真实信息的含义。从本质上来看,信息对抗是在信息熵的保护或打击层面上讨论问题,也就是围绕着信息的利用来进行对抗。

在我国全国计算机信息系统安全保护工作由公安部主管。国家安全部、国家保密局和国务院其他有关部门,负责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定。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。

1.2 安全威胁

1.2.1 安全威胁的概念及其分类

1. 安全威胁的概念

安全威胁是指对安全的一种潜在的侵害。威胁的实施称为攻击。一般认为,目前计算机系统安全面临的威胁主要分为3类:信息泄露、拒绝服务、信息破坏。其中信息泄露、信息破坏也可能造成系统拒绝服务。

① 信息泄露:指敏感数据在有意或无意中被泄露出去或丢失,它通常包括:信息在传输中丢失或泄露(如利用电磁泄漏或搭线窃听等方式可截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析,推导出有用信息);信息在存储介质中丢失或泄露;通过建立隐蔽信道窃取敏感信息等。

② 信息破坏:以非法手段获得对数据的使用权,删除、修改、插入或重发某些信息,以取得有益于攻击者的响应信息;恶意添加,修改数据,以干扰用户的正常使用。

③ 拒绝服务:如执行无关程序使系统响应减慢甚至瘫痪,影响正常用户的使用,甚至使合法用户被排斥而不能得到相应的服务。

安全威胁可能来自多个方面。影响、危害计算机系统安全的因素分为自然因素和人为因素两类。

自然因素包括:各种自然灾害,如水、火、雷、电、风暴、烟尘、虫害、鼠害、海啸和地震等;系统的环境和场地条件,如温度、湿度、电源、地线和其他防护设施;电磁辐射和电磁干扰;硬件设备自然老化,可靠性下降等。

人为因素又有无意和故意之分。人为无意的破坏包括操作失误(操作不当、误用媒体、设置错误)、意外损失(电力线搭接、电火花干扰)、编程缺陷(经验不足、检查漏项、不兼容文件)、意外丢失(被盗、被非法复制、丢失媒体)、管理不善(维护不利、管理松弛)、无意破坏(无意损坏、意外删除等)。人为故意的破坏包括敌对势力、各种计算机犯罪。

2. 安全威胁的分类

(1) 从威胁的来源看可分为内部威胁和外部威胁

① 内部威胁:由于内部人员对机构的运作、结构熟悉,导致内部攻击不易被发觉,内部人员