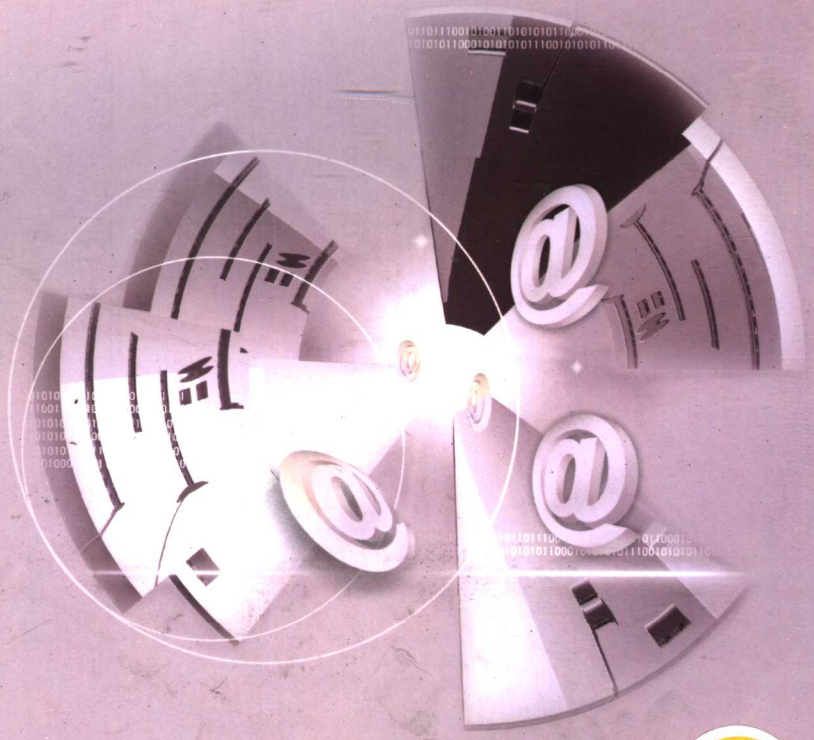
高等院校信息安全专业规划教材

计算机系统安全原理与技术

- 计算机系统安全问题及安全机制
- 应急响应与灾难恢复
- 计算机安全等级评测

提供电子教案

陈 波 于 泠 肖军模 编著
宋如顺 审



机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

计算机系统安全原理与技术

陈 波 于 泠 肖军模 编著
宋如顺 审

机 械 工 业 出 版 社

本书全面介绍了计算机系统可能存在的安全问题和普遍采用的安全机制，包括计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全、应急响应与灾难恢复、计算机系统安全风险评估、计算机安全等级评测与安全管理等内容。

本书还对各种安全技术实践作了指导，帮助读者理解并掌握相关安全原理，提高信息安全防护意识和安全防护能力。本书每章都有习题。

本书可以作为信息安全专业、信息对抗专业、计算机专业、信息工程专业或相近专业的本科和研究生教材，也可以作为网络信息安全领域的科技人员与信息系统安全管理员的参考书。

图书在版编目（CIP）数据

计算机系统安全原理与技术/陈波等编著.—北京：机械工业出版社，2006.1
（高等院校信息安全专业规划教材）
ISBN 7-111-17893-9

Ⅰ.计… Ⅱ.陈… 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(2005)第134862号

机械工业出版社(北京市百万庄大街22号 邮政编码 100037)
策　　划：胡毓坚
责任编辑：车　忱
责任印制：洪汉军
北京原创阳光印业有限公司印刷
2006年1月第1版·第1次印刷
787mm×1092mm 1/16·22.5印张·558千字
0001—5000册
定价：31.00元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：(010)68326294
封面无防伪标均为盗版

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

随着计算机技术的不断发展和网络的日益普及，人们对计算机和网络的依赖也越来越强。计算机信息系统，无论是在单机系统、局域网还是在广域网系统中，都存在着自然和人为等诸多因素的脆弱性和极大的安全威胁。针对计算机信息系统的攻击与破坏事件层出不穷，如果不进行及时和正确的保护，这些攻击与破坏事件轻则会干扰人们的日常生活，重则会造成巨大的经济损失，甚至威胁国家的安全。所以，信息系统的安全问题已引起世界各国的高度重视，人们不惜投入大量的人力、物力和财力来提高计算机信息系统的安全性。

在高等教育领域大力推进信息安全的专业化教育，是国家在信息安全领域掌握自主权、占领先机的重要举措。办好信息安全本科专业的第一要务是拥有高质量的教材。为此，2004 年 3 月 10 日在解放军信息工程大学召开了高等院校信息安全专业规划教材编委会第一次工作会议，会上确立了第一批教材的选题，其中包括《计算机系统安全原理与技术》。

本书是以在解放军理工大学通信工程学院和南京师范大学讲授过 4 年的《计算机系统安全原理与技术》教学讲义为基础编写而成的。编写中我们力求做到：

内容的系统性

本书内容包括计算机系统可能存在的安全问题和普遍采用的安全机制，包括计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全以及安全管理和安全立法。

根据信息保障模型(PDRR)——防护、检测、反应与恢复的概念，本书还包括了应急响应与灾难恢复、计算机系统安全风险评估、计算机安全等级评测与安全管理等章节，使得全书的体系更加完整。

原理的经典性

在选材上，我们尽量选择成熟的和长期起作用的计算机系统安全理论与最新的研究成果，避免选择那些时效性很强的具体技术与方法。根据这些想法，我们广泛综合了国内外有关信息安全论著中的理论与素材以及我们自己的实际工作经验，论述了计算机硬件、操作系统、计算机网络、数据库系统和应用系统各个层次上的信息安全原理。

技术的先进性

信息安全技术随着计算机和网络通信等技术的发展而发展，针对不断出现的安全问题，人们还在不断完善和提出解决问题的方法和技术。因而，本书在相应章节介绍了这些改进后的或新提出的技术内容。如在第 5 章网络安全中，不仅介绍了入侵检测技术，还介绍了目前正在成为研究热点的入侵防御技术；在第 8 章应急响应与灾难恢复中介绍了当前入侵追踪的最新研究成果；在第 10 章中介绍了我国信息安全法律法规体系中的一个重要内容——今年 4 月 1 日开始执行的《中华人民共和国电子签名法》以及 5 月 30 日起实施的《互联网著作权行政保护办法》。

技术的实践性

本书作为信息安全专业或相近专业的教材，不仅应达到理论正确、先进，文字通顺、流畅等标准，还应具备对技术实践的指导作用。为此，本书结合已经完成的国家 863 应急项目以及多项省级科研项目的研究实践和作者多年的教学实践，对学生进行的各种安全技术实践作了指

导。如在第2章中介绍了利用MD5算法设计一个数据文件完整性检测程序的方法，利用BMP图像文件进行信息隐藏的实现方法；第4章给出了Windows 2000/XP系统的安全配置方案；第6章给出了SQL Server 2000安全管理实例；第7章给出了缓冲区溢出贬程实例，以及Web安全设置的方法；第8章介绍了网站备份与恢复系统的开发过程；第9章介绍了Cyber-Cop Scanner安全评估工具的使用，并给出了信息系统安全风险评估的一个实例。通过这些实践环节，学生可以深刻理解并掌握相关安全原理，提高信息安全防护意识和安全防护能力。

书中1.2、3.1、4.2、5.1、5.8、6.2、7.4等节由肖军模教授编写，其余章节由陈波、于泠共同完成。本书在写作过程中，查阅、参考了大量的文献、资料，限于篇幅未能在书后的参考文献中一一列出，在此一并致谢。

在整个写作过程中，全军信息安全研究中心主任、解放军理工大学通信工程学院肖军模教授从书稿大纲的确定到书稿的审定倾注了大量的心血；江苏省保密技术工程研究中心主任、南京师范大学计算机系宋如顺教授也审阅了书稿。在此致以衷心的感谢。

随着网络通信技术、计算机技术的不断发展，计算机系统安全仍是一个不断发展的研究领域。我们对这一领域的研究还不很深，虽然我们力求达到以上的目标，书中一定还存在错误和不足之处，恳请广大读者和专家提出批评和改进意见。

为了配合教学，本书还提供了与教材配套的电子教案，读者可在机械工业出版社网站www.cmpbook.com上免费下载。

作　者

目　录

第 1 章　计算机系统安全概论

本章首先介绍计算机信息系统面临的主要安全威胁，并指出安全问题的根源，然后介绍信息安全概念的发展以及计算机系统安全研究的主要内容。

1.1　计算机信息系统面临的安全威胁

1.1.1　计算机信息系统

按照我国颁布的《计算机信息系统安全保护等级划分准则》的定义，“计算机信息系统是由计算机及其相关的配套设备、设施(含网络)构成的，按照一定的应用目标和规格对信息进行采集、加工、存储、传输、检索等处理的人机系统。”

实际上，我们所讨论的典型的计算机信息系统，应该是在计算机网络环境下运行的信息处理系统。计算机信息系统由硬件与软件支撑系统和使用人员两部分组成。

硬件系统包括组成计算机、网络的硬件设备及其他配套设备。软件系统包括操作平台软件、应用软件和应用业务软件。操作平台软件通常指操作系统和语言及其编译系统；应用平台软件通常指支持应用开发的软件，如数据库管理系统及其开发工具，各种应用编程和调试工具等；应用业务软件是指专为某种应用而开发的软件。

众多的计算机信息系统，从应用角度可分为两类：一类是以客户机/服务器模式运行的信息系统，重点是提供信息服务，如 Web 网信息系统等；另一类是以信息交换模式运行的信息系统，重点是进行信息交换，如电子商务信息系统等。不论是何种应用模式，计算机信息系统的最终服务对象是人，人是计算机信息系统的设计者、使用者，而计算机信息系统的安全问题也主要由各类人员引入，使用人员由合法使用人员和非法使用人员组成。

1.1.2　安全威胁

20 世纪 40 年代，随着计算机的诞生，计算机安全问题也随之产生。20 世纪 70 年代以来，随着计算机的广泛应用，以计算机网络为主体的信息处理系统迅速发展。同以前的计算机安全保密相比，计算机信息系统的安全问题要多得多，也复杂得多，涉及物理环境、硬件、软件、数据、传输、体系结构等多个方面。

威胁信息系统安全的因素是多方面的，目前还没有统一的方法对各种威胁加以区别和进行准确的分类。而且不同威胁的存在及其重要性是随环境的变化而变化的。下面是对现代信息系统及网络通信系统常遇到的一些威胁及其来源的简单介绍。

正常的信息流向应当是从合法发送端源地址流向合法接收端目的地址，如图 1-1 所示。

1. 中断威胁

如图 1-2 所示，中断威胁使正在使用的信息系统毁坏或不能使用，即破坏了可用性(Availability)。

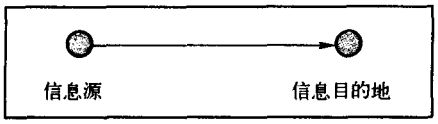


图 1-1　正常的信息流向

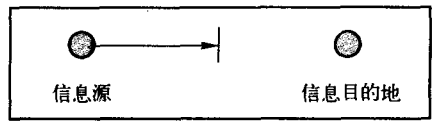


图 1-2　中断威胁

攻击者可以从下列几个方面破坏信息系统的可用性：

- 使合法用户不能正常访问网络资源。
- 使有严格时间要求的服务不能及时得到响应。
- 摧毁系统。物理破坏网络系统和设备组件使网络不可用，或者破坏网络结构使之瘫痪等。如硬盘等硬件的毁坏，通信线路的切断，文件管理系统的瘫痪等。

最常见的中断威胁是造成系统的拒绝服务，即信息或信息系统资源的利用价值或服务能力下降或丧失。

2. 截获威胁

如图 1-3 所示，截获威胁是指一个非授权方介入系统，使得信息在传输中被丢失或泄露的攻击，它破坏了保密性(Confidentiality)。非授权方可以是一个人、一个程序或一台计算机。

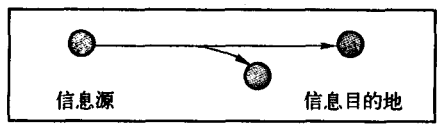


图 1-3　截获威胁

这种攻击主要包括：

- 利用电磁泄露或搭线窃听等方式可截获机密信息，通过对信息流向、流量、通信频度和长度等参数的分析，推测出有用信息，如用户口令、账号等。
- 文件或程序的不正当复制。

3. 篡改威胁

如图 1-4 所示，篡改威胁以非法手段窃得对信息的管理权，通过未授权的创建、修改、删除和重放等操作，使信息的完整性(Integrity)受到破坏。

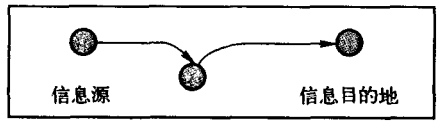


图 1-4　篡改威胁

这些攻击主要包括：

- 改变数据文件，如修改信件内容等。
- 改变程序使之不能正确执行。

4. 伪造威胁

如图 1-5 所示，在伪造威胁中一个非授权方将伪造的客体插入系统中，破坏信息的真实性(Authenticity)。例如在网络中插入假信件，或者在文件中追加记录等。

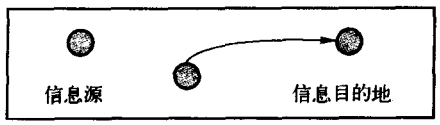


图 1-5　伪造威胁

1.1.3　安全问题的根源

前面介绍了信息系统常见的安全威胁，下面从物理安全问题、软件组件的缺陷、系统的安全漏洞、TCP/IP 协议的安全和人的因素等几个方面分析这些安全问题的根源。

1. 物理安全问题

计算机系统物理方面的安全主要表现为物理可存取、电磁泄露等方面的问题。此外，物理安全问题还包括设备的环境安全、位置安全、限制物理访问、物理环境安全和地域因素等。由于这种问题是设计时所遗留的固有问题，一般除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。

2. 软件组件

软件组件可分为操作平台软件、应用平台软件和应用业务软件三类，以层次结构构成软件组件体系。操作平台软件处于基础层，它维系着系统硬件组件协调运行的平台，因此平台软件的任何风险都可能直接危及、转移或传递到应用平台软件。

应用平台软件处于中间层次，它是在操作平台支撑下运行的支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可以直接危及或传递给应用业务软件。

应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险，都直接表现为信息系统的风险。

随着软件系统规模的不断增大，软件组件中的安全漏洞或“后门”也不可避免地存在，这也是信息安全问题的主要根源之一。比如我们常用的操作系统，无论是 Windows 还是 UNIX，几乎都存在或多或少的安全漏洞，众多的各类服务器（典型的如微软的 IIS 服务器）、浏览器、数据库管理系统、一些桌面软件等都被发现过存在安全漏洞。可以说任何一个软件系统都会因为程序员的一个疏忽、设计中的一个缺陷等而存在漏洞，

3. 网络和通信协议

人们在享受因特网技术给全球信息共享带来的方便性和灵活性的同时必须认识到，因特网及其通信协议栈在开放网络环境下，其安全隐患是全面而系统的。基于 TCP/IP 协议栈的因特网及其通信协议存在很多的安全问题。支持因特网运行的 TCP/IP 协议栈在设计的当初原本只考虑了互联互通和资源共享的问题，并未考虑也无法兼容解决来自网络的大量安全问题。

4. 人的因素

人是信息活动的主体，人的因素其实是影响信息安全问题的最主要因素。

（1）人为的无意失误。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

（2）人为的恶意攻击。人为的恶意攻击也就是黑客攻击。攻击又可以分为以下两类：一

类是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。由于现在还缺乏针对网络攻击的卓有成效的反击和跟踪手段，使得许多黑客攻击的隐蔽性好、杀伤力强。

(3) 管理上的因素。网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于安全方面的管理。此外，管理的缺陷还可能出现在系统内部，例如内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄漏，从而为一些不法分子制造了可乘之机。

1.1.4 计算机信息系统的安全需求

计算机信息系统的安全需求主要有：保密性、完整性、可用性、可控性、不可抵赖性和可存活性等。

1. 保密性(Confidentiality)

保密性表示对信息资源开放范围的控制，不让不应涉密的人接触秘密信息。实现保密性的方法一般是通过信息的加密、对信息划分密级，并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。除了考虑数据加密、访问控制外，还要考虑计算机电磁泄露可能造成的信息泄露。

2. 完整性(Integrity)

完整性需求即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。信息的完整性是信息安全的基本要求。破坏信息的完整性是影响信息安全的常用手段。目前对于动态传输的信息，许多协议确保信息完整性的方法大多是收错重传、丢弃后续包。但黑客的攻击可以改变信息包内部的内容。

3. 可用性(Availability)

可用性是指信息可被合法用户访问，按要求的权限使用而不遭拒绝服务。例如，在网络环境下破坏网络和有关系统的正常运行，就属于对可用性的攻击。信息的可用性与保密性之间存在一定的矛盾。系统为了控制非法访问可以采取许多安全措施，但系统不应该阻止合法用户对系统中信息的利用。

4. 可控性(Controllability)

可控性是指对信息的内容及传播具有控制能力。任何信息都要在一定传输范围内可控，如密码的托管政策。托管政策即将加密算法(或后门)交由第三方或第四方管理，在使用时要严格按有关管理规定执行。

5. 不可抵赖性(Non-repudiation)

不可抵赖性通常又称为不可否认性，是指信息的发送者无法否认已发出的信息，信息的接收者无法否认已经接收的信息。否认是指通信的某一方出于某种目的而出现下列抵赖行为：

- 发信者事后否认曾经发送过某些消息。
- 收信者事后否认曾经接收过某些消息。
- 发信者事后否认曾经发送过某些消息的内容。
- 收信者事后否认曾经收到过某些消息的内容。

不可否认性措施主要有：数字签名，可信第三方认证技术等。