重点大学计算机专业系列教材

信息安全技术基础和安全策略

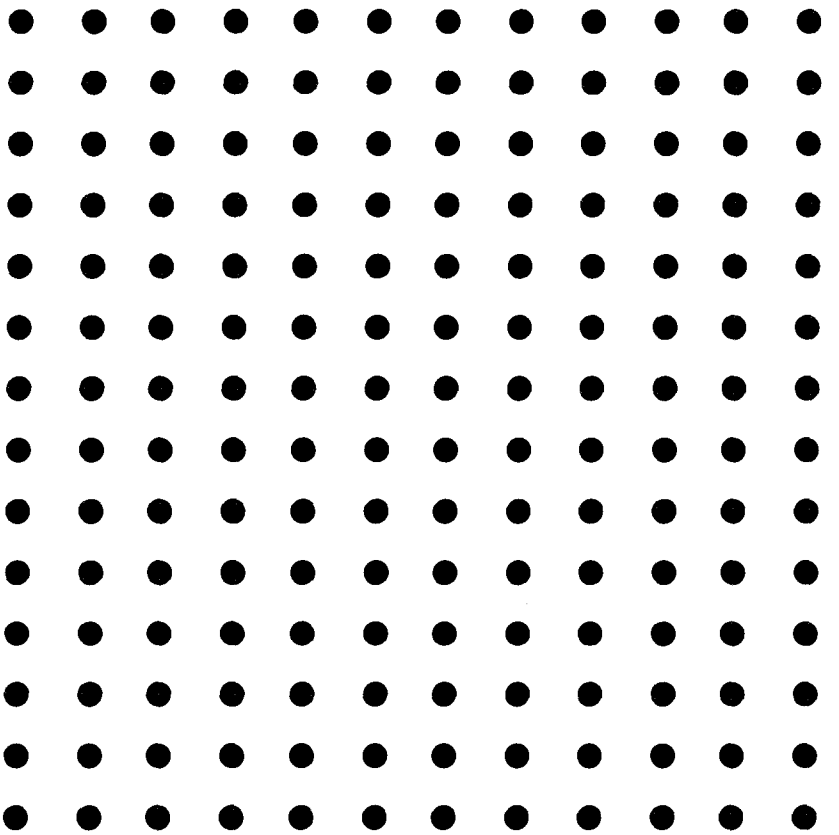
薛质 苏波 李建华 编著

清华大学出版社

重点大学计算机专业系列教材

信息安全技术基础和安全策略

薛质 苏波 李建华 编著



清华大学出版社
北京

内 容 简 介

随着科技的发展，以计算机和通信技术为代表的信息技术和相关产业得到了巨大的成功。在网络与信息的大量应用中，安全正面临着前所未有的挑战。信息安全已经成为一个综合的工程，也将成为一个新兴的研究学科。

本书旨在阐述网络与信息安全的基础知识，使读者了解信息安全技术的主要内容、法律法规和相关标准、安全策略，加强对信息安全重要性的认识，提高信息安全防范意识。希望本书能对我国还有待发展的网络与信息安全起到促进作用，并满足广大计算机爱好者对计算机网络安全知识的迫切需求。本书既可以作为高等学校信息安全专业学生的教材，也可以作为“信息安全专业人员认证联盟(ISPCC)”的培训教材。

全书的主要内容包括信息安全定义、法律法规和标准，信息安全威胁，信息安全策略和对策，操作系统安全和风险评估，网络安全威胁和防范，常见数据库安全，信息安全防范主流技术简介，病毒防治和灾难恢复，安全管理。

图书在版编目(CIP)数据

信息安全技术基础和安全策略/薛质，苏波，李建华编著. —北京：清华大学出版社，2007.4
(重点大学计算机专业系列教材)
ISBN 978-7-302-14087-0

Ⅰ. 信…　Ⅱ. ①薛… ②苏… ③李…　Ⅲ. 信息系统－安全技术－高等学校－教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2006)第 130217 号

责任编辑：丁　岭　顾　冰
责任校对：李建庄
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京国马印刷厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：15.5　**字　数**：382 千字
版　　次：2007 年 4 月第 1 版　　**印　次**：2007 年 4 月第1 次印刷
印　　数：1～3000
定　　价：24.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：023057-01

INTRODUCTION

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

2. 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系；基本教材与辅助教材以及教学参考书的关系；文字教材与软件教材的关系，实现教材系列资源配套。

5. 依靠专家，择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

FOREWORD

前言

计算机网络(以下简称网络)近几年在我国有了很快的发展。在网络的大量应用中,安全问题正面临着前所未有的挑战。信息安全将成为一个新兴的研究学科,它需要我们在网络安全领域进行长期的研究和攻关。

网络的基础在于资源的共享。自由,一直以来是网络的基本准则。随着 Internet 的迅速发展,网络上的资源共享越来越被强化,随之而来的,是越来越突出的网络安全问题。

目前,Internet 已遍及世界上 240 个国家和地区,每时每刻都为用户提供着各种类型的信息服务。随着技术的飞速发展,Internet 的服务已经日益呈现出多样化的特征,除了最初的电子邮件、万维网外,在 Internet 中出现了越来越多的集视频、声音、数据于一体的服务,如视频会议、网络电话等。

现在的社会是高度信息化的社会,计算机已经被应用到政治、军事、金融、商业、交通、电信、教育等行业。人们在日常的生活中对计算机的依赖程度大大提高,尤其是近年来国家实施的信息系统工程和信息基础设施建设,已经使计算机信息系统成为当今社会特征的一个重要组成部分。越来越多的各类信息管理系统,收集和储存了大量的个人私密资料和信息。而这些信息的处理和交换都无一例外地将通过计算机网络来完成。毫不夸张地说,网络已经成为人们获取信息的一个重要途径,正日益改变着人的生活方式。随着网络的不断发展,网络的资源共享性、开放性、交换性日益增强,各种原来不可能实现的业务都在网络上出现了。电子货币、数字签名、电子商务、政务上网、网络银行,使得人们可以在家中完成一切商业交易。各类银行网络的建设,更是使资金的异地流通变得快捷方便了。这也带来了巨大的安全隐患和风险。

计算机犯罪已经成为一种新的高智能犯罪,它具有高度的隐蔽性,给社会带来了巨大的危害,也给侦破带来了一定的麻烦。同时,由于计算机网络的广泛互联和无地域性特征,使得罪犯可以轻松地实施异地甚至是跨国的犯罪和资金转移。

“黑客”，一个神秘的带着传奇色彩的称呼。他们像是网络世界中的侠客，打抱不平，凭借着高超的技术在网络世界自由驰骋，没有什么可以阻拦他们，他们崇尚高度的、绝对的自由。在很多的学生和青少年心中，他们是神圣的象征。据调查，有 60% 以上的青少年网络用户梦想成为一个“黑客”。在信息化高度发展的美国，重要部门每天都发生着大量的入侵事件，造成上亿美圆的经济损失。通过计算机盗取信用卡信息、修改学习成绩、篡改网站首页，已经是很平常的事情。

在我国，仅 1998 年报道的黑客事件就不下五起，大量的网站页面被篡改，工作人员的账户和密码被窃取。由于网络入侵的隐蔽性，还有很多的入侵至今没有被发现。有的入侵即使被发现了，出于诸多原因，受害方也不愿意对外公布。据有关部门统计，利用计算机网络窃取商业机密的事件正以每月 260% 的速度增加着。而据专家估计，公开报道的入侵事件大约只占入侵事件的 0.2%。

“在网上，没有人知道你是谁”，这是一个漫画上的说明文字。它反映了网络的不可信原则。在网络上，没有事情是可以被绝对相信的，即使是一封非常明确的来信，也极有可能是伪造的。网络安全，已经成为一个最受关注的话题，它已不仅是学术研究者的研究方向，而成为了全球 Internet 用户所关注的热点。

多年来，黑客对计算机信息系统的攻击一直就没有停止过，其手段也越来越高明，从最初的猜测用户密码、利用计算机软件缺陷，发展到现在的通过操作系统源代码分析操作系统漏洞。同时人们还发现，网络的普及使得攻击工具和代码更容易被一般用户获得，这无疑给网络安全带来了更大的挑战。

解决网络安全问题，任重而道远。

本书内容由浅入深，介绍了网络安全和计算机信息系统安全的相关知识。阅读本书可以了解中国计算机信息系统的安全现状、网络安全产生的隐患和风险来源、风险给计算机信息系统运行带来的危害以及具体的安全防护措施和技术。

本书部分内容涉及网络结构、网络协议等知识点，读者应具备基本的网络操作技能并对网络结构及网络协议有基本的了解。

编　者

2007 年 1 月

于上海交大

CONTENTS

目录

CHAPTER 1

第1章 信息安全概述

信息一直以来都是全人类的宝贵资源。各种功能的信息系统，已经成为推动社会发展前进的催化剂和加速器。同时，由于计算机网络（以下简称网络）的快速普及，处理信息的多样性也使得计算机成为了人类社会中一个不可或缺的工具，正日益为社会各个行业和部门的生产和管理提供有效的帮助，其提供的多种信息服务，给人类带来了便捷的生活方式。例如与我们关系密切的金融业的信息化进程，使资金流动加快，清算资料的速度大大提高，异地的资金划转也变得十分快捷了。可以说，信息化和计算机网络把人和人、国和国的距离缩短了。

信息与信息系统的安全现已成为一个新兴的学科，信息安全管理已经成为公共安全的重要组成部分。信息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、应用数学等多种学科的边缘学科。随着全球信息化的发展，国家之间的“距离”越来越近，计算机网络在带来了众多快捷、便利的服务的同时也带来了新的危害。如何解决信息安全问题，如何制止计算机犯罪，如何建立安全的网络体系，已经成为全球关注的焦点。解决信息安全问题，已经是迫在眉睫的事情了。

网络的安全措施一般分为三大类：逻辑上的、物理上的和政策上的。面对安全的种种威胁，仅仅依靠物理上的和政策（法律）上的手段来有效防止计算机犯罪显得十分有限和困难，因此必须使用逻辑上的措施，即研究开发有效的网络安全技术，如安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其完整性和保密性；防止非法用户（程序）的侵入，限制网络上用户（程序）的访问权限，保证信息存放的私有性。除此之外，一个安全的计算机网络还必须考虑通信双方的身份真实性和信息的可用性。

网络安全就是要保证网络上存储和传输信息的安全性。由于网络设计之初，只考虑了方便性和开放性，这使得网络非常脆弱，容易受到黑客的攻击或有组织的入侵，也会由于系统内部人员的不规范操作和恶意行为，

使网络信息系统遭受破坏，导致信息泄露或丢失。为了解决这个问题，国内外的研究机构在这方面做了很多工作，在数据加密技术、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡(存储、加密、智能卡)、拒绝服务、入侵侦测、网络安全性分析、信息内容安全监测和信息安全标准化等方面做了大量的研究和相关开发工作。

1.1 什么是信息安全

广义的信息安全是指防止信息财产被故意的或偶然的非授权泄露、更改、破坏，或防止信息被非法辨识、控制，即确保信息的保密性、可用性、完整性、可控性。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、加密与鉴别等七个方面。

狭义的信息安全指网络上的信息安全，也称为网络安全，它所涉及的领域也是相当广泛的。简单地说，网络中的安全是指一种能够识别和消除不安全因素的能力。

信息安全的定义随着应用环境的改变也有不同的诠释。对用户来说，个人隐私和机密数据的传输受到机密性、完整性和安全性的保护，避免他人窃取资料是他们的安全要求。而对安全保密部门来说，过滤非法的、有害的或涉及国家机密的信息，成为其信息安全的重点。在下面的相关内容中，我们将对信息安全的具体表现做进一步说明。

网络安全与其保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动或静态存放时不被未授权用户非法访问，但允许授权用户访问。显然，网络安全、信息安全和系统安全的研究领域是相互交错和关联的。

1.2 网络安全和黑客

一直以来，黑客是具有传奇色彩的崇尚自由的一群人，然而黑客行为造成的损失却是巨大的。据 CERT(计算机紧急事件响应小组)的调查显示，约 20%的网站都遭受过安全侵害，每年在美国由安全导致的损失可达 100 亿美圆。根据有关调查，大部分的入侵和安全事件的威胁并非来源于外部，而是来源于网络内部的破坏。虽然网络安全已经被全球的人们所重视，各大公司、机构也都纷纷建立了自己的安全策略，设置并使用了防病毒、防火墙、入侵侦测系统(IDS)以及跟踪和记录网络活动的程序，但仍然不足以阻止攻击的产生。原因在于黑客的攻击比起前几年来越来越复杂，技术上越来越先进；超负荷的 IT 技术人员和由于侥幸心理所导致的资金投入的缺口，使得专业安全技术人员不能获得更多的资源；最重要的一点是大量的没有严密安全保护的系统正在全球快速地被部署并投入使用。

黑客的分类有很多种标准，一般以黑客的行为态度和动机来划分，有以下三类。

(1) 偶然的破坏者。顾名思义，这类人喜欢进入他人的系统，但不一定有明确目标，多数情况下是恶作剧。大部分黑客属于这一类。

(2) 坚定的破坏者。这类黑客的入侵都带有明确的目标，并会给系统带来巨大的甚至是毁灭性的破坏。

（3）间谍。窃取商业资料或情报，获得信息或摧毁服务，对资源不加限制地访问。

1.3　计算机信息系统面临的安全威胁、攻击及其脆弱性

网络所提供的资源共享性、用户使用的方便性、分布处理提高效率的特性以及可扩充性，在一定程度上大大增加了网络受攻击的可能性。现今的计算机网络面临着各式各样的威胁和人为攻击，而计算机系统本身，无论是在存取与运行的基本原理上，或者是系统本身的设计、技术、结构、工艺等方面都存在着一些有待弥补的缺陷。或者可以这样说，计算机信息系统本身的脆弱性，使其成为被攻击的目标或被利用为有效的攻击手段。

1.3.1　计算机信息系统面临的安全威胁

网络的安全威胁来自众多方面，或者说，计算机信息系统本身的脆弱性，使其成为被攻击的目标。网络安全威胁可导致信息的保密性、完整性、可用性降低，从而造成经济损失。当前网络安全威胁主要有以下几个方面。

- 自然灾害、人为事故。由于自然灾害和人为的事故造成的威胁，如天灾、硬件故障、工作人员误操作等。
- 计算机犯罪。利用暴力或非暴力，故意破坏计算机中的机密信息，以及危害计算机实体和信息安全的不法行为，如数据欺骗、特洛伊木马等。
- 黑客行为。黑客的入侵或干扰，比如非法访问、拒绝服务等。
- 内部破坏。内部人员对计算机系统的破坏或泄密。
- 电子情报。通过信息窃取、流量分析、监听等手段获取信息资源。
- 信息战。为了军事目的，获取或干扰他国的信息和信息系统。
- 计算机病毒。制造、传播和利用计算机病毒进行破坏计算机信息系统的行为。如常见的蠕虫病毒（“求职信”、“红色代码”、Nimda、“震荡波”、“冲击波”等）。需要特别注意的是，现在的很多病毒都已经具备了部分黑客软件的特征。

1.3.2　计算机信息系统受到的攻击

对信息的人为故意的威胁称为攻击。攻击按威胁和攻击的对象可分为两类：一类是对计算机信息系统实体的威胁和攻击；另一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包括了对计算机系统实体和信息两个方面的威胁和攻击。

对计算机信息系统实体的威胁和攻击主要指对计算机及其外部设备和网络的威胁和攻击。对信息系统实体的威胁和攻击不仅会造成财产损失，还会使信息系统遭受破坏。

对信息的威胁和攻击主要有以下两种。

（1）信息泄露，指偶然的或故意的获得（窃取或分析破译）目标系统的信息，特别是敏感信息。

（2）信息破坏，指由于偶然事故或人为破坏，使信息的正确性、完整性和可用性受到破坏，使系统的信息被修改、删除、添加、伪造或非法复制，造成大量信息的破坏、修改或丢失。

就攻击方式来说，攻击可归纳为主动攻击和被动攻击两类。