

高等院校信息安全专业系列教材

网络安全

胡道元 摇 闵京华 摇 编著

清华大学出版社
北京

内 容 简 介

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力拒绝服务或被非授权使用、篡改。

全书共分 源篇 圆章,全面讲述网络安全的基础知识(网络安全的入门和基础)、网络安全体系结构(开放系统互连安全体系结构和 陈测康安全体系结构)、网络安全技术(防火墙、灾 陈测康黑客技术、漏洞扫描、入侵检测、恶意代码与计算机病毒的防治、系统平台安全以及应用安全),以及网络安全工程(网络安全设计、管理、评估)。

本书内容翔实,结构合理,概念清楚,语言精炼,实用性强,易于教学。

本书可作为信息安全、计算机、通信等专业本科生、硕士生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

网络安全 胡道元,闵京华编著—北京:清华大学出版社, 圆园园圆

(高等院校信息安全专业系列教材)

陈只身 陈只身 陈只身 陈只身

I 援网...摇 II 胡... ② 闵...摇 III 援计算机网络 原安全技术 原高等学校 原教材摇 IV 援陈只身 陈只身

中国版本图书馆 CIP 数据核字(圆园园圆)第 缘园缘园号

出 版 者:清华大学出版社

地 址:北京清华大学学研大厦

邮 政 编 码:缘园园园

邮 编:缘园园园

社 总 机:园园园园园园园园

客 户 服 务:园园园园园园园园

组稿编辑:张摇民

文稿编辑:王冰飞

封面设计:摇摇摇

印 刷 者:摇摇摇摇摇摇

装 订 者:摇摇摇摇摇摇

发 行 者:新华书店总店北京发行所

开 本:员缘园伊圆缘园伊圆缘园 印张:猿猿 字 数:缘园园千字

版 次:圆园园圆年 员月第 员版 圆园园圆年 员月第 员次印刷

书 号:陈只身 陈只身 陈只身 陈只身 缘园缘园

印 数:员~ 圆园园圆

定 价:园园园园元

高等院校信息安全专业系列教材

编审委员会

名誉主编：何德全(中国工程院院士)

主摇摇任：肖国镇

委摇摇员：(按姓氏笔画为序)

方滨兴摇 冯登国摇 刘建亚摇 何大可摇 张玉清
杨摇波摇 吴摇刚摇 李建华摇 张焕国摇 陈克非
宫摇力摇 洪佩琳摇 胡振辽摇 胡铭曾摇 胡道元
侯整风摇 卿斯汉摇 钱德沛摇 曹珍富摇 谢冬青
焦金生摇 廖明宏摇 裴昌幸

策划编辑：张摇民

本书责任编委：方滨兴

序

摇摇在社会信息化的进程中,信息已成为社会发展的重要资源,信息安全也成为 21 世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益,各国政府都非常重视信息和网络安全,信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展,国家领导高度重视,各部门通力合作、统筹规划,大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展,社会对信息安全人才的需求在不断增加,在高等教育领域大力推进信息安全的专业化教育,将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前,许多大学和科研院所已创办了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度,认真组织全国各高校和科研院所的专家、学者,共同研讨信息安全专业的教育方法和课程体系,并在进行大量前瞻性研究工作的基础上,启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材,相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去,也希望这套教材能够取得成功并不断完善,以促进各高等院校培养出更多、更好的信息安全专门人才,为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士
高等院校信息安全专业系列教材编审委员会名誉主编

2004年 苑月于北京

出版说明

21世纪是信息时代,信息已成为社会发展的重要战略资源,社会的信息化已成为当今世界发展的潮流和核心,而信息安全在信息社会中将扮演极为重要的角色,它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展,国家对信息安全人才的需求量不断增加,但目前信息安全人才极度匮乏,远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾,必须加快信息安全人才的培养,以满足社会的需求。为此,教育部继1998年批准在武汉大学开设信息安全本科专业之后,又批准了多所高等院校设立信息安全本科专业,而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科,对于这一新兴学科的培养模式和课程设置,各高校普遍缺乏经验,因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动,并成立了“高等院校信息安全专业系列教材”编审委员会,由我国信息安全领域著名专家何德全院士担任名誉主编,著名学者肖国镇教授担任编委会主任,共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则,认真研讨国内外高等院校信息安全专业的教学体系和课程设置,进行了大量前瞻性的研究工作,而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定,确定了编写教材的作者,这些作者绝大多数都是既在本专业领域有深厚的学术造诣,又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材,其特点是:

- ① 体系完整,结构合理,内容先进。
- ② 适应面广,能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。
- ③ 立体配套,除主教材外,还配有多媒体电子教案、习题与实验指导等。
- ④ 版本更新及时,紧跟科学技术的新发展。

为了保证出版质量,我们坚持宁缺毋滥的原则,成熟一本,出版一本,并保持不断更新,力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材,满足学生用书的基础上,还经由专家的推荐和审定,遴选了一批国外信息安全领域优秀的教材加入到本系列教材中,以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍,同时也欢迎广大读者提出宝贵意见,以便我们对本系列教材的组织、编写与出版工作不断改进,为我国信息安全专业的教材建设与人才培养做出更大的贡献。

我们的联系地址是:北京电报大楼,清华大学出版社,联系人:张民。

中国计算机学会教育专业委员会
清华大学出版社
2008年 苑月

摇摇我们生存的世界并不安宁,人们渴望有一个安全、和平的生存空间,随着信息技术的发展,特别是网络的发展,人们的诸多活动越来越多地依赖于网络空间,然而,网络空间并非总是安全的。

当前我国的网络安全正面临着严峻的挑战。一方面随着电子政务工程的启动、电子商务的开展以及国家关键基础设施的网络化,网络安全的需求更加严格和迫切。另一方面,黑客攻击、病毒传播以及形形色色的网络攻击日益增加,网络安全防线十分脆弱。

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力拒绝服务或被非授权使用、篡改。

从本质上讲,安全就是风险管理,风险是构成安全基础的基本观念。风险是丢失需要保护的资产的可能性,是威胁和漏洞的综合结果。没有漏洞的威胁就没有风险,而没有威胁的漏洞也没有风险。

“网络安全”是信息安全专业的主要专业课,学生应从以下三个方面掌握网络安全的基本原理、主要技术以及解决方案:

(员) 网络安全体系结构

由开放系统互连模型和 ~~网络安全~~ 层次体系结构决定了网络安全体系结构的层次模型。网络安全体系结构描述网络信息体系结构在满足安全需求方面各基本元素之间的关系,反映信息系统安全需求和网络体系结构的共性。并由此派生了相应的网络安全协议、技术和标准。

(圆) 网络安全技术

单一的网络安全技术和网络安全产品无法解决网络安全的全部问题。应根据应用需求和安全策略,综合运用各种网络安全技术,包括防火墙、~~入侵检测~~、~~病毒扫描~~、~~入侵检测~~、~~恶意代码~~、~~与计算机病毒~~的防治、系统平台安全以及应用安全等。

(猿) 网络安全工程

对网络安全进行的综合处理,要从体系结构的角度,用系统工程的方法,贯穿网络安全设计、开发、部署、运行、管理和评估的全过程。

本书共分源篇圆章。第员篇为网络安全基础知识,共缘章,是网络安全的入门和基础。第圆篇为网络安全体系结构,共圆章,讲述开放系统互连安全体系结构和网络安全体系结构。第猿篇为网络安全技术,共怨章,讲述各种网络安全技术。第源篇为网络安全工程,共源章,分别讲述网络安全设计、管理、评估。

每章开始列出本章要点,最后给出小结,概要地总结本章的要点。每章结尾附有习题,帮助读者复习。

本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

本书由胡道元教授主编并编著了第员章~第苑章、第员苑第员愿和第员章,闵京华博士编著了第员源第员远和第员章,朱卫国编著了第员章,邵忠岗、黄新民、刘旺泉、陆新宇、邢羽嘉分别编著了第愿章~第员章。赵青为书稿的编排、打印做了大量的工作。闵京华博士做了全书的最后校订工作。

作摇者
圆园年 苑月

目 录

第 1 篇 网络安全基础知识

第 1 章 引论	猿
1.1 网络安全概述	猿
1.1.1 网络安全的概念	猿
1.1.2 网络安全的属性	苑
1.1.3 网络安全层次结构	愿
1.1.4 网络安全模型	怨
1.2 安全的历史回顾	员
1.2.1 通信安全	员
1.2.2 计算机安全	圆
1.2.3 网络安全	猿
1.3 网络安全处理	源
1.3.1 网络安全综合处理	源
1.3.2 网络安全处理过程	远
1.4 密码学	苑
1.4.1 密码学的基本原理	苑
1.4.2 对称密钥密码技术	愿
1.4.3 公钥密码技术	怨
1.5 本章小结	圆
习题	圆
第 2 章 风险分析	圆
2.1 资产保护	圆

- 摇摇摇 摇摇摇资产的类型 圆
- 摇摇摇 摇摇摇潜在的攻击源 猿
- 摇摇摇 摇摇摇资产的有效保护 原
- 圆 圆 圆 攻击 缘
 - 圆 圆 圆 攻击的类型 缘
 - 圆 圆 圆 主动攻击和被动攻击 苑
 - 圆 圆 圆 访问攻击 苑
 - 圆 圆 圆 篡改攻击 猿
 - 圆 圆 圆 拒绝服务攻击 猿
 - 圆 圆 圆 否认攻击 猿
- 圆 圆 圆 风险管理 猿
 - 圆 圆 圆 风险的概念 猿
 - 圆 圆 圆 风险识别 猿
 - 圆 圆 圆 风险测量 猿
- 圆 圆 圆 本章小结 猿
- 习题 源

- 第 猿 章 安全策略 源
 - 猿 猿 猿 安全策略的功能 源
 - 猿 猿 猿 安全策略的类型 源
 - 猿 猿 猿 信息策略 源
 - 猿 猿 猿 系统和网络安全策略 猿
 - 猿 猿 猿 计算机用户策略 猿
 - 猿 猿 猿 访问控制策略 源
 - 猿 猿 猿 邮件策略 源
 - 猿 猿 猿 用户管理程序 源
 - 猿 猿 猿 系统管理程序 源
 - 猿 猿 猿 应急响应程序 源
 - 猿 猿 猿 配置管理程序 源
 - 猿 猿 猿 设计方法 缘
 - 猿 猿 猿 灾难恢复计划 缘
 - 猿 猿 猿 安全策略的生成、部署和有效使用 缘
 - 猿 猿 猿 安全策略的生成 缘
 - 猿 猿 猿 安全策略的部署 缘

猿猿猿摇安全策略的有效使用	猿猿
猿猿猿摇本章小结	猿猿
习题	猿猿
第 源章 网络信息安全服务	猿源
猿源猿摇机密性服务	猿源
猿源猿猿摇文件机密性	猿源
猿源猿猿摇信息传输机密性	猿源
猿源猿猿摇通信流机密性	猿源
猿源猿摇完整性服务	猿源
猿源猿猿摇文件完整性	猿源
猿源猿猿摇信息传输完整性	猿源
猿源猿摇可用性服务	猿源
猿源猿猿摇后备	猿源
猿源猿猿摇在线恢复	猿源
猿源猿猿摇灾难恢复	猿源
猿源猿摇可审性服务	猿源
猿源猿猿摇身份标识与身份鉴别	猿源
猿源猿猿摇网络环境下的身份鉴别	猿源
猿源猿猿摇审计功能	猿源
猿源猿摇数字签名	猿源
猿源猿摇运输层鉴别	猿源
猿源猿摇公钥基础设施	猿源
猿源猿摇访问控制	猿源
猿源猿摇本章小结	猿源
习题	猿源
第 缘章 网络安全处理	猿缘
猿缘猿摇评估	猿缘
猿缘猿猿摇网络评估	猿缘
猿缘猿猿摇物理安全评估	猿缘
猿缘猿猿摇策略和过程评估	猿缘
猿缘猿猿摇预防措施评估	猿缘

苑园猿摇网络地址转换	苑园猿
苑园源摇合作伙伴网络	苑园源
苑园缘摇网络安全层次模型	苑园缘
苑园远摇第二层保护的网路——链路层安全	苑园远
苑园愿摇第三层保护的网路——网络层安全	苑园愿
苑园赧摇传输层保护的网路	苑园赧
苑园园摇应用层安全性	苑园园
苑园员摇宰宰宰 应用安全技术	苑园员
苑园圆摇韵韵韵安全体系到 裁裁裁安全体系的映射	苑园圆
苑园猿摇本章小结	苑园猿
习题	苑园猿

第猿篇摇网络安全技术

第愿章 防火墙	苑缘
愿园摇防火墙的原理	苑缘
愿园员摇防火墙的概念	苑缘
愿园圆摇防火墙的功能	苑远
愿园猿摇边界保护机制	苑苑
愿园源摇潜在的攻击和可能的对象	苑愿
愿园缘摇互操作性要求	苑愿
愿园远摇防火墙的局限性	苑愿
愿园愿摇防火墙的分类	苑园
愿园园摇防火墙的访问效率和安全需求	苑园
愿园员摇防火墙技术	苑员
愿园圆摇包过滤技术	苑员
愿园猿摇应用网关技术	苑圆
愿园源摇状态检测防火墙	苑圆
愿园缘摇电路级网关	苑猿
愿园远摇代理服务器技术	苑猿
愿园愿摇防火墙体系结构	苑源
愿园园摇双重宿主主机体系结构	苑源

愿被屏蔽主机体系结构 员缘

愿被屏蔽子网体系结构 员远

愿堡垒主机 员愿

愿数据包过滤 员愿

 愿数据包过滤的特点 员愿

 愿数据包过滤的应用 员怨

 愿过滤规则制定的策略 员员

 愿数据包过滤规则 员猿

愿状态检测的数据包过滤 员源

愿防火墙的发展趋势 员苑

愿本章小结 员愿

习题 员怨

第 怨章 灾晕 员园

怨灾晕概述 员园

 怨灾晕的概念 员园

 怨灾晕的类型 员员

 怨灾晕的优点 员猿

怨灾晕技术 员猿

 怨灾晕密码技术 员猿

 怨灾晕身份认证技术 员缘

 怨灾晕隧道技术 员缘

 怨灾晕密钥管理技术 员远

怨第二层隧道协议——蕴云孕栽孕和蕴栽孕 员远

 怨灾晕隧道协议的基本概念 员远

 怨灾晕蕴云 员愿

 怨灾晕孕栽孕 员愿

 怨灾晕蕴栽孕 员园

 怨灾晕孕栽孕和蕴栽孕的比较 员猿

怨第三层隧道协议——员礁云 员源

怨本章小结 员远

习题 员远

第 10 章 陈陈糟	100
陈陈糟安全体系结构	100
陈陈糟的概念	100
陈陈糟的功能	100
陈陈糟本系结构	100
安全联盟和安全联盟数据库	100
安全策略和安全策略数据库	100
陈陈糟运行模式	100
陈陈糟安全协议——粤匀	100
粤匀概述	100
粤匀头部格式	100
粤匀运行模式	100
数据完整性检查	100
陈陈糟安全协议——耘孕	100
耘孕概述	100
耘孕头部格式	100
耘孕运行模式	100
陈陈糟陈陈云云协议	100
陈陈云云概述	100
陈陈云云包头部格式	100
陈陈云云载荷头部	100
陈陈云云载荷	100
陈陈云云协商阶段	100
交换类型	100
陈陈糟陈陈云云协议	100
陈陈云云概述	100
陈陈云云交换模式	100
本章小结	100
习题	100
第 11 章 黑客技术	100
黑客的动机	100
黑客攻击的流程	100

摇摇摇摇踩点	摇摇
摇摇摇摇扫描	摇摇
摇摇摇摇查点	摇摇
摇摇摇摇获取访问权	摇摇
摇摇摇摇权限提升	摇摇
摇摇摇摇窃取	摇摇
摇摇摇摇掩盖踪迹	摇摇
摇摇摇摇创建后门	摇摇
摇摇摇摇拒绝服务攻击	摇摇
摇摇摇摇黑客技术概述	摇摇
摇摇摇摇协议漏洞渗透	摇摇
摇摇摇摇密码分析还原	摇摇
摇摇摇摇应用漏洞分析与渗透	摇摇
摇摇摇摇社会工程学	摇摇
摇摇摇摇恶意拒绝服务攻击	摇摇
摇摇摇摇病毒或后门攻击	摇摇
摇摇摇摇针对网络的攻击	摇摇
摇摇摇摇拨号和 灾 攻击	摇摇
摇摇摇摇针对防火墙的攻击	摇摇
摇摇摇摇网络拒绝服务攻击	摇摇
摇摇摇摇本章小结	摇摇
习题	摇摇

第 摇摇章 漏洞扫描	摇摇
摇摇摇摇计算机漏洞	摇摇
摇摇摇摇摇摇计算机漏洞的概念	摇摇
摇摇摇摇摇摇存在漏洞的原因	摇摇
摇摇摇摇摇摇公开的计算机漏洞信息	摇摇
摇摇摇摇实施网络扫描	摇摇
摇摇摇摇发现目标	摇摇
摇摇摇摇攫取信息	摇摇
摇摇摇摇漏洞检测	摇摇
摇摇摇摇常用的网络扫描工具	摇摇

不同扫描策略	本章小结	习题
第 4 章 入侵检测	入侵检测概述	入侵检测的概念
入侵检测系统的结构	入侵检测系统分类	基于主机的入侵检测系统
基于网络的入侵检测系统	基于内核的入侵检测系统	两种入侵检测系统的结合运用
分布式的入侵检测系统	入侵检测系统的分析方式	异常检测技术——基于行为的检测
误用检测技术——基于知识的检测	异常检测技术和误用检测技术的比较	其他入侵检测技术的研究
入侵检测系统的设置	入侵检测系统的部署	基于网络入侵检测系统的部署
基于主机入侵检测系统的部署	报警策略	入侵检测系统的优点与局限性
入侵检测系统的优点	入侵检测系统的局限性	本章小结
习题	第 5 章 恶意代码与计算机病毒的防治	恶意代码
	恶意代码的概念	