

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787302179634

10位ISBN编号：7302179638

出版时间：2008-10

出版时间：清华大学出版社

作者：胡道元，闵京华 编著

页数：482

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全>>

前言

网络安全，尤其是Internet安全正面临着严重的挑战，一方面是Internet规模的扩大和关键应用的激增，因而对网络安全的需求很高；另一方面是网络安全攻击的持续增加、安全漏洞的增长，使实施网络安全的难度大大增加。

从网络安全体系结构的观点看，不同类型的漏洞、攻击、威胁存在于网络的不同层次。

层次的方案深入研究网络环境的各种技术及每一层次的每种技术的复杂性。

第2版充实了Internet安全体系结构的内容，更新了一些网络安全技术及网络安全管理技术。

具体有以下几点：（1）第1章增加了一节网络安全挑战,论述了当前网络安全形势。

（2）第5章改为安全体系结构，论述了系统安全体系结构、OSI安全体系结构及网络安全体系结构。

（3）第2篇改为Internet安全体系结构，论述了依照层次结构的原则，对不同类型的攻击实施不同层的保护。

（4）更新了第11-13章及第15章部分内容。

（5）参照新公布的ISO/IECFDIS18028重新编写了第19章网络安全管理。

本书共分4篇20章。

第1篇为网络安全基础知识，共5章，是网络安全的入门和基础知识。

第2篇为Internet安全体系结构，共2章，讲述依照Internet层次结构的原则，对不同类型的攻击实施不同层的保护。

第3篇为网络安全技术，共9章，讲述各种网络安全技术。

第4篇为网络安全工程，共4章，分别讲述网络安全设计、管理和评估。

每章开始列出本章要点，每章最后一节给出小结，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、计算机和通信等专业本科生和研究生的教科书，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1-7章、第17、18和20章，闵京华博士编著了第14、16和19章，朱卫国编著了第15章，陆新宇、邢羽嘉编著了第11-13章。

黄新民、刘旺泉编著了第8-10章。

网络安全（第2版）第2版前言参与第2版编写的有胡道元（第1章、第5-7章）、闵京华（第19章）、朱卫国（第15章）、陆新宇（第11-13章）。

胡道元于北京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）和信息的信息处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

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：（1）网络安全体系结构由开放系统互连模型和Internet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。

<<网络安全>>

(2) 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、VPN、IPSec、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、系统平台安全及应用安全等。

(3) 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4篇20章。

第1篇为网络安全基础知识,共5章,是网络安全的入门和基础。

第2篇为网络安全体系结构,共2章,讲述开放系统互连安全体系结构和Internet安全体系结构。

第3篇为网络安全技术,共9章,讲述各种网络安全技术。

第4篇为网络安全工程,共4章,分别讲述网络安全设计、管理、评估。

网络安全(第2版)第1版前言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1章-第7章、第17、第18和第20章,闵京华博士编著了第14、第16和第19章,朱卫国编著了第15章,邵忠岩、黄新民、刘旺泉、陆新宇、邢羽嘉分别编著了第8章-第13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。

<<网络安全>>

内容概要

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）和信息的信息处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

全书共分4篇20章，全面讲述网络安全的基础知识（网络安全的入门和基础），Internet安全体系结构（依照Internet层次结构的原则，对不同类型的攻击实施不同层的保护），网络安全技术（防火墙、VPN、IPSec、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、系统平台及应用安全）及网络安全工程（网络安全设计、管理和评估）。

本书内容翔实，结构合理，概念清楚，语言精练，实用性强，易于教学。

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

作者简介

胡道元，清华大学教授、著名计算机网络及网络安全专家、我国计算机网络的开拓者，被国内外业界誉为“中国Internet之父”，研究成果多次获得国家科技进步奖和国际大奖，编著了十余本计算机网络及网络安全的著作，在国内外发表了百余篇论文。

<<网络安全>>

书籍目录

第1篇 网络安全基础知识 第1章 引论 第2章 风险分析 第3章 安全策略 第4章 网络信息安全服务
第5章 网络安全处理第2篇 网络安全体系结构 第6章 开放系统互连安全体系结构 第7章 Internet安
全体系结构第3篇 网络安全技术 第8章 防火墙 第9章 VPN 第10章 IPSec 第11章 黑客技术 第12章
漏洞扫描 第13章 入侵检测 第14章 恶意代码与计算机病毒的防治 第15章 系统平台安全 第16章
应用安全第4篇 网络安全工程 第17章 安全需求分析 第18章 安全基础设施设计原理 第19章 安全管
理 第20章 安全认证和评估附录 各章习题答案参考文献

章节摘录

插图：第1篇 网络安全基础知识第1章 引论1.2 安全的历史回顾随着社会和技术的进步，信息安全也有一个发展的过程，了解信息安全的发展历史，可使人们更全面地解决当前遇到的各种信息安全问题。

粗略地，可把信息安全分成3个阶段，即通信安全（comsec）、计算机安全（compusec）和网络安全（netsec）。

1.2.1 通信安全早期，所有的资产都是物理的，重要的信息也是物理的，如古代刻在石头上，到后来写在纸上。

为了保护这些资产，只需要用墙、护城河、警卫等物理安全措施。

信息传递通常由信使完成，需要时可带有警卫。

除非用物理的掠夺，否则就无法得到信息。

但是，物理安全存在缺陷，如果报文在传递中被截获，则报文的信息就会被敌人知悉。

因此就产生了通信安全的问题。

早在公元前600年Julius Caesar生成了Caesar密码，以使报文即使被截获也无法读出。

这个概念一直延续到第二次世界大战，德国人使用一种称为Enigma的机器来加密报文，用于军队，当时他们认为Enigma是不可破译的。

确实是这样，如果使用恰当，要破译它非常困难。

但经过一段时间发现，由于某些操作员的使用差错，Enigma被破译了。

军事通信也使用编码技术，将每个字编码后放入报文传输。

在战争期间，日本人曾用编码后的字通信，即使美国人截获了这些编码也难以识别该报文。

在准备Midway之战时，日本人曾传送编码后的报文，使日美之间在编码和破译方面展开了一场有关通信安全的对抗。

为了防止敌人窃听语音报文，美国军队曾使用一种Navaho码的步话机，Navaho用本土语言传送报文，敌人即使收听到无线电通信，也无法懂得报文的意思。

第二次世界大战后，苏联间谍曾经使用一次填充来保护传递的信息。

一次填充的方法是在每一页上用带有随机数的文字填充，每一页只用一个报文。

这个加密方案如果使用正确则难以破译。

但是由于他们的使用方法不正确（重用一次填充），结果某些报文被破译出来。

从上面这些事例可知，通信安全的主要目的是解决数据传输的安全问题，主要的措施是密码技术。

<<网络安全>>

编辑推荐

《网络安全(第2版)》内容翔实，结构合理，概念清楚，语言精练，实用性强，易于教学。

《网络安全(第2版)》可作为信息安全、计算机和通信等专业本科生和研究生的教科书，也可供从事相关专业的教学、科研和工程人员参考。

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）和信息的信息处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>