高等院校信息与通信工程系列教材

通信网的安全理论与技术

戴逸民　王培康　陈巍　编著

清华大学出版社

高等院校信息与通信工程系列教材

通信网的安全理论与技术

戴逸民　王培康　陈巍　编著

清华大学出版社
北京

内容简介

本书主要阐述网络可能存在的13种信息安全隐患(窃听、修改、重放、伪装、哄骗、渗透、抵赖、拒绝服务、计算机病毒、因特网蠕虫、特洛伊木马、黑客后门、黑客入侵),以及为了克服安全隐患,在网络上实现网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移时,网络需要解决的6类信息安全策略或安全机制(信息的隐蔽、信息的完整性、信息的认证、信息的访问控制、信息的电磁泄露控制、网络的防御策略)和6种信息安全技术(信息加密、信息认证、抵御计算机病毒、被动的网络防御、主动的网络防御、数字产品版权保护)。

本书的特点是:内容新颖,概念清晰,实践性强,突出新技术,许多内容,特别是安全可靠的防火墙攻防模型、计算机资源保护模型、主动的网络防御技术、抵御已知攻击能力的分析方法和双层数字水印算法等,都是信息与通信工程领域的基础理论与较为前沿的专业知识,具有广泛的应用前景。

本书可作为高等院校通信工程、信息安全及计算机专业本科生和硕士研究生的教材,也可作为计算机和通信领域专业技术人员的参考书。

图书在版编目(CIP)数据

通信网的安全理论与技术/戴逸民,王培康,陈巍编著. —北京:清华大学出版社,2006.7
(高等院校信息与通信工程系列教材)
ISBN 7-302-12624-0

Ⅰ.通…　Ⅱ.①戴…②王…③陈…　Ⅲ.通信网—安全技术—高等学校—教材　Ⅳ.TN915.08

中国版本图书馆CIP数据核字(2006)第016208号

出 版 者:清华大学出版社
http://www.tup.com.cn
社 总 机:010-62770175
地　　址:北京清华大学学研大厦
邮　　编:100084
客户服务:010-62776969
组稿编辑:陈国新
特邀编辑:魏艳春　曾德斌
印 装 者:清华大学印刷厂
发 行 者:新华书店总店北京发行所
开　　本:185×260　**印张**:29.75　**字数**:701千字
版　　次:2006年7月第1版　2006年7月第1次印刷
书　　号:ISBN 7-302-12624-0/TN·311
印　　数:1～3000
定　　价:39.00元

出版说明

信息与通信工程学科是信息科学与技术的重要组成部分。改革开放以来，我国在发展通信系统与信息系统方面取得了长足的进步，形成了巨大的产业与市场，如我国的电话网络规模已占世界首位，同时该领域的一些分支学科出现了为国际认可的技术创新，得到了迅猛的发展。为满足国家对高层次人才的迫切需求，当前国内大量高等学校设有信息与通信工程学科的院系或专业，培养大量的本科生与研究生。为适应学科知识不断更新的发展态势，他们迫切需要内容新颖又符合教改要求的教材和教学参考书。此外，大量的科研人员与工程技术人员也迫切需要学习、了解、掌握信息与通信工程学科领域的基础理论与较为系统的前沿专业知识。为了满足这些读者对高质量图书的渴求，清华大学出版社组织国内信息与通信工程国家级重点学科的教学与科研骨干以及本领域的一些知名学者、学术带头人编写了这套高等院校信息与通信工程系列教材。

该套教材以本科电子信息工程、通信工程专业的专业必修课程教材为主，同时包含一些反映学科发展前沿的本科选修课程教材和研究生教学用书。为了保证教材的出版质量，清华大学出版社不仅约请国内一流专家参与了丛书的选题规划，而且每本书在出版前都组织全国重点高校的骨干教师对作者的编写大纲和书稿进行了认真审核。

祝愿《高等院校信息与通信工程系列教材》为我国培养与造就信息与通信工程领域的高素质科技人才，推动信息科学的发展与进步做出贡献。

北京邮电大学

陈俊亮

前　言

自从1956年第一个计算机网络建立以来，网络技术得到了极其迅速的发展，使我们的生活方式和工作方式发生了巨大变化。这些新的变化主要包括网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移等。

因特网核心协议(TCP/IP)是按照自由开放和彼此信任的群体使用来设计的，在当前的现实环境下却表现出内在缺陷。它们虽然能很好地完成互联层(IP层)和传输层的功能，但也存在不少可被攻击者利用来进行攻击的“漏洞”。

本书概述网络可能存在的13种信息安全隐患和在网络上实现网上通信、网上无纸办公、网上使用信用卡、网上签订合同、网上购物、电子现金转移时，为了克服安全隐患网络需要解决的6类信息安全策略或安全机制和6种信息安全技术。

(1) 网络可能存在的13种信息安全隐患是：窃听、修改、重放、伪装、哄骗、渗透、抵赖、拒绝服务、计算机病毒、因特网蠕虫、特洛伊木马、黑客后门、黑客入侵。

(2) 网络需要解决的6类信息安全策略或安全机制是：信息的隐蔽、信息的完整性、信息的认证、信息的访问控制、信息的电磁泄露控制、网络的防御策略。

(3) 网络常用的6种信息安全技术是：信息加密、信息认证、抵御计算机病毒、被动的网络防御、主动的网络防御、数字产品版权保护。

本书是作者在中国科学技术大学研讨班(Seminar)课程——“通信网的安全理论与技术”4年的教学实践的基础上编写而成。

本书可作为高等院校通信工程、信息安全及计算机专业本科生和硕士研究生的教材，也可作为计算机和通信领域专业技术人员的参考书。

全书分为11章，下面概括介绍每章的内容。

第1章扼要介绍网络的组网原理及可能存在的13种信息安全隐患。

第2章从信息安全原理的层次结构、物理概念、数学方法、实际应用和实现技巧等角度阐述6类信息安全对策或安全机制。

第3章给出5个信息加密范例和7个密文破译范例，以此说明信息加密与密文破译的重要概念和通用原理。

第4章概述密钥流产生原理、技术和实例。

第5章以高级加密标准AES为例，概述分组密码设计原理、技术和抵御已知攻击的强度。

第6章概述双密钥思想的优势和缺陷，指出弥补缺陷的途径；简介广义数字签名的概念和算法。

第7章阐述通信网安全认证协议、网络安全认证协议和用于认证的典型算法。

第 8 章简介网络分层结构、控制报文协议(ICMP)和 TCP 连接规程,分别叙述它们的漏洞和对策,最后构造一个安全可靠的防火墙攻防模型,并概括叙述网络防御技术的发展方向。

第 9 章简介计算机安全等级、操作系统发展与恶意代码的演化关系,分别叙述 4 种恶意代码的入侵机制和防御措施,最后构造一个安全可靠的计算机资源保护模型。

第 10 章从密码算法的选择、操作模式的选择、使用环境的考虑、不同品牌安全设备的互连等方面,叙述网上安全通信系统设计的指导思想,并给出 3 个实例。

第 11 章简介空间和频谱数字水印嵌入原理及提取技术,分别叙述它们的优势和漏洞,最后构造一个安全可靠的双层数字水印算法,适用于"可信赖的"数码相机和摄像机等。

本书的第 1 章、第 2 章(2.1～2.3 节)、第 7 章由王培康编写,第 2 章(2.4～2.7 节)、第 3 章～第 6 章、第 8 章～第 10 章由戴逸民编写,第 11 章由陈巍编写。张曦、杨婧和储元麟参与 11.5 节"用于数码相机的双层数字水印算法"的实验工作。戴逸民负责全书的统稿。

作者于合肥中国科学技术大学

2005 年 10 月

daiym@ustc.edu.cn

目　录

第 1 章　通信网面临的安全威胁

首先简介因特网的安全目标(资源保护)、安全威胁、安全系统特征、安全策略和安全系统密级层次划分方法,然后仔细分析因特网两项应用服务所面临的安全威胁,并扼要介绍其他通信网的组网工作原理和面临的安全威胁。

1.1　因特网的安全隐患与安全处理方法

越来越多的单位、团体、公司开始依赖因特网完成办公、管理、商务、通信和协作。与过去相比,现在敏感信息的完整性和在线通信日臻重要。对病毒和黑客作出反应是任何网络管理工作的一个主要职责。本节将简介因特网的安全隐患与安全处理方法。

1.1.1　资源保护

在计算机网络中,安全可以定义为由网络管理员进行的一系列处理,以保证信息只在经认证的用户之间共享。当设计和执行一项安全计划时,首先需要了解所要保护的资源。

1. 保护资源的重要性

因特网是一个开放的网络,因此,内置的保护信息的能力是非常差的。从安全观点看,因特网天生就不安全。保护敏感的数据,只允许经过授权的人员使用它,这是使用因特网所面临的挑战。

2. 用户或单位需要保护的资源

用户或单位需要保护的资源,由以下四部分组成,如图 1-1 所示。

(1) 本地资源

基于口令保护的屏幕保护程序能阻止侦听。当从因特网下载任何文件时,需要每一个使用者使用病毒检验程序,并观察有关警告。

(2) 网络资源

用于整个单位的主要通信媒体是网络和它的资源。如果一个黑客得到某个网络访问和控制权,那么他便能访问该单位的大部分网络数据。

(3) 数据库和信息资源

任何单位的主要资源是组织起来的或分散的信息。黑客的最终目标是发现这些信