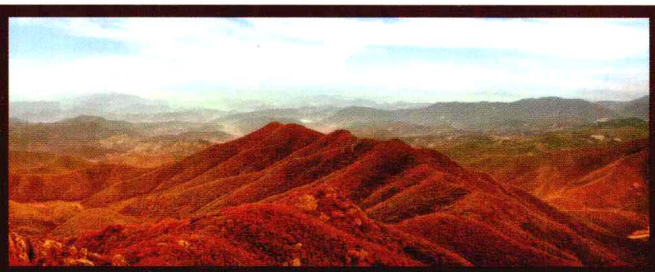
高等学校信息安全类专业系列教材

网络安全与管理



□ 陈红松 编著

清华大学出版社
北京交通大学出版社

高等学校信息安全类专业系列教材

网络安全与管理

陈红松　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书介绍计算机网络安全与管理技术，是面向信息安全与计算机专业的教材。本书首先从整体上介绍了网络安全与管理的基本概念、产生背景、特点及设计原则，从系统工程的角度介绍了网络安全管理的体系结构。从网络攻击技术出发，逐层次介绍了网络安全与管理的相关技术理论与标准规范。本书共分13章，内容包括网络安全与管理概述、相关规范、网络攻击与安全评估、网络安全的密码学基础、身份认证与网络安全、防火墙技术、VPN技术、入侵检测技术、面向内容的网络信息安全、电子商务安全、无线网络安全技术、网络管理原理与技术及网络信息安全的法律法规体系。

本书既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材，也可作为网络安全管理工程技术人员的参考书。

图书在版编目(CIP)数据

网络安全与管理/陈红松编著. —北京：清华大学出版社；北京交通大学出版社，2010.10
(高等学校信息安全类专业系列教材)
ISBN 978－7－81123－743－6

Ⅰ. ①网… Ⅱ. ①陈… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第181802号

责任编辑：谭文芳　　特邀编辑：王志刚
出版发行：清华大学出版社　　邮编：100084　　电话：010－62776969　　http://www.tup.com.cn
　　北京交通大学出版社　　邮编：100044　　电话：010－51686414　　http://press.bjtu.edu.cn
印 刷 者：北京瑞达方舟印务有限公司
经　　销：全国新华书店
开　　本：185×260　　印张：20.25　　字数：518千字
版　　次：2010年10月第1版　　2010年10月第1次印刷
书　　号：ISBN 978－7－81123－743－6/TP·624
印　　数：1～3 000册　　定价：33.00元

前　言

随着计算机和网络通信技术的快速发展，网络的开放性、互连性、共享程度的提高，来自外部的黑客攻击和内部的威胁使网络安全及管理问题日益突出，网络安全正面临重大挑战。本书首先介绍了网络安全与管理的基本概念、产生背景、特点及设计原则，从系统工程的角度介绍了网络安全管理的体系结构，分析了构建网络安全管理体系的必要性，注重各安全技术之间的相互作用与联系；从网络攻击技术出发，逐层次介绍了网络安全与管理的相关技术理论与标准规范。本书紧密结合当前网络信息安全领域的发展动态，体现学科前沿和研究成果，并且注重一定的实践性和创新性，每章后面都有相应习题供学生总结和复习所学知识，兼顾知识体系的完整性与系统性，本书很多内容来自编者的科研工程项目及课堂教学实践。

本书共分13章。第1章介绍网络安全与管理的基本概念、产生背景、特点及设计原则；第2章介绍网络安全与管理的体系规范与标准；第3章介绍网络攻击的概念，网络风险的识别与安全评估方法；第4章介绍网络安全的密码学基础；第5章介绍网络安全所涉及的身份认证技术与相关协议；第6章介绍防火墙的概念与原理、指标与选型、发展趋势等；第7章介绍虚拟专用网的关键技术及发展趋势，其中包括基于不同协议的VPN技术等；第8章介绍入侵检测与防护系统的关键技术以及蜜罐蜜网技术等；第9章介绍了面向内容的网络安全监控技术，并给出了论坛类网站内容安全监控模型；第10章介绍了电子商务中的安全机制以及安全电子商务协议；第11章介绍了无线网络安全技术，包括移动Ad hoc网络及无线传感器网络的安全机制；第12章介绍了网络管理原理及技术，包括SNMP/OSI网络管理框架以及新型网络管理模型；第13章介绍了网络信息安全的法律法规体系及国内外网络安全立法框架。

本书既可作为高等院校信息安全、计算机等相关专业的本科生和研究生相关课程的教材，也可作为网络安全管理工程技术人员的参考书。

本书由北京科技大学计算机系陈红松副教授主持全书内容的组织策划和统稿编写工作，黄小莉博士参与编写了其中的第4章和第10章。北京科技大学的王昭顺教授、张晓彤教授、北京邮电大学的杨义先教授、哈尔滨工业大学的傅忠传副教授等为本书的编写提供了许多宝贵建议，北京科技大学的研究生黄木、王艺璇等也参与了部分资料的收集及部分图表的制作，本书得到网络与交换技术国家重点实验室（北京邮电大学）开放课题资助（编号SKLNST－2008－1－12），中国博士后科学基金第46批资助（编号20090460245），国家自然科学基金资助（编号90818016），作者在此致以深切的感谢。

由于网络安全与管理技术发展更新较快，作者水平有限，书中的不足之处在所难免，殷切希望广大读者批评指正并提出宝贵建议和意见，以便进一步完善教材内容。编者E-mail：architecture_ustb@yahoo.com.cn。

编　者

2010年4月

目　录

第 1 章　网络安全与管理概述与规划

本章要点：

- ☑ 网络安全与管理的基本概念及意义
- ☑ 网络安全问题的产生背景
- ☑ 网络安全与管理的特点
- ☑ 网络安全与管理的设计原则
- ☑ 网络安全管理规划设计与实施案例

1.1　网络安全与管理概述

网络是信息社会的基础，它已经广泛深入到社会、经济、政治、文化、军事、生活等各个领域，成为人们生活中不可缺少的一部分。但由于因特网的开放性等因素，它也带来了很多安全问题，如机密信息被窃听和篡改、网络黑客攻击、计算机蠕虫病毒等，由此带来的损失和影响是巨大的。本书从网络安全与管理的角度系统阐述了相关技术及特点，并给出了一些实施案例。

1.1.1　网络安全与管理的基本概念

随着计算机和通信技术的发展，国家和社会的信息化程度逐步提高，网络已成为全球信息基础设施的主要组成部分，成为现代人工作生活中必不可少的一部分，人们对网络的依赖程度也逐步加深，一旦网络由于种种原因发生故障，陷于瘫痪，人们的生活也必然会受到极大的影响。网络技术如同一把双刃剑，在带给我们便利的同时，所引发的安全隐患问题也很值得我们关注。广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，它涉及安全体系结构、安全协议、密码理论、信息内容分析、安全监控、应急处理等。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。如何更有效地保护重要的信息数据、提高网络系统的安全性已经成为所有网络应用必须考虑和解决的问题之一。

有效的网络管理不仅局限于技术上的问题，同时也是管理和法律法规的问题。网络监管系统的基础设备要采用先进的硬件设备，包括防毁、防电磁信息辐射泄露、抗电磁干扰、数据灾备及电源保护等设备。网络安全技术随着现代技术的进步不断发展，如果没有合理有效的网络管理，就难以有健康发展的网络环境。从管理上来说，目前成立专门的监管部门，分

区域分行业进行监督和管理。网络监管还必须从法律法规上进行强化，制定规范的法律法规，并达成行业和相关人员的自律。网络技术的进步给了人们以更大的信息支配能力，互联网打破了传统的区域性，使个人的网络行为对社会发生的影响空前增大，也要求人们更严格地控制自己的行为。要建立一个洁净的互联网，需要的不仅是技术、法律和管理上的不断完备，还需要网络中每个信息人的自律和自重，用个人的网络伦理道德和内在价值标准来约束自己的行为，从而自觉维护网络社会的和谐发展。

1.1.2 网络安全与管理的定义

本节给出了网络安全与管理的定义，以及网络管理的功能。

1. 网络安全的定义

国际标准化组织（International Organization for Standardization，ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此，可以将计算机网络安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。网络安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从广义上说，网络安全包括网络硬件资源和信息资源的安全性，而硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等，要实现信息快速、安全的交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性和真实性等是网络安全研究的重要课题。

网络安全包括一切解决或缓解计算机网络技术应用过程中存在的安全威胁的技术手段或管理手段，也包括这些安全威胁本身及相关的活动。网络安全的具体含义会随着重视“角度”的变化而变化。例如，从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读、写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务以及网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。网络安全性就是保护网络程序、数据或者设备，使其免受非授权使用或访问，它的保护内容包括：信息和资源、客户和用户，以及私有性。

在不同的环境和应用中，网络安全的解释也不完全相同。

① 运行系统安全，即保证信息处理和传输系统的安全，多数是指操作系统安全。

② 网络上系统信息的安全，包括口令鉴别、用户存取权限控制、安全审计、计算机病毒防治和数据加密等。

③ 网络上信息传播的安全，即信息传播后的安全。

④ 网络上信息内容的安全是信息安全在法律、政治、道德层次上的要求。

⑤ 网络上信息本身的安全，即我们讨论的狭义的“网络安全”，其侧重于保护网络信息

的保密性、真实性和完整性。

⑥ 物理安全，即网络中各种物理设备的安全，主要是指防盗、防火、防静电、防雷击以及防电磁泄露。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务以及网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行有效控制。因此，网络信息安全是一个系统工程，必须综合采取各种措施才能奏效。

在网络连接能力、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、网络应用安全和网络管理的安全等。因此网络安全问题，应该做到防范于未然。有时不会想到自己会成为目标的时候，威胁就已经出现了，一旦发生，常常令人措手不及，造成极大的损失。

2. 网络管理的定义

网络管理就是指监督、组织和控制网络通信服务，以及信息处理所必需的各种活动的总称。其目标是确保计算机网络的持续正常运行，并在计算机网络运行出现异常时能及时响应和排除故障。一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行。

网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，二者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理，即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部计算机、服务器、交换机等进行管理；对行为的管理，即针对用户的使用进行管理；对资产的管理，即统计软硬件的信息等。

国际标准化组织在 ISO/IEC 7498—4 中定义并描述了开放系统互联（Open System Interconnection，OSI）管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互联管理是指这样一些功能，它们控制、协调、监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。通常对一个网络管理系统需要定义以下内容。

① 系统的功能：即一个网络管理系统应具有哪些功能。

② 网络资源的表示：网络管理很大一部分是对网络中资源的管理。网络中的资源就是指网络中的硬件、软件以及所提供的服务等，而一个网络管理系统必须在系统中将它们表示出来，才能对其进行管理。

③ 网络管理信息的表示：网络管理系统对网络的管理主要靠系统中网络管理信息的传递来实现。网络管理信息应如何表示、怎样传递、传送的协议是什么？这都是一个网络管理系统必须考虑的问题。

④ 系统的结构：即网络管理系统的结构是怎样的。

3. 网络管理的功能

国际标准化组织定义网络管理有五大功能：故障管理、配置管理、性能管理、安全管