WANGLUO ANQUAN GAILUN

网络安全概论

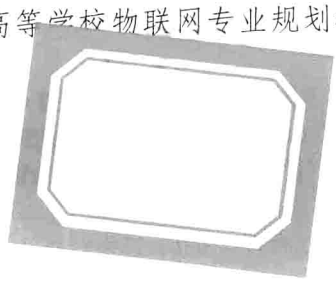
何小东　陈伟宏　彭智朝　编著






清华大学出版社
http://www.tup.com.cn
北京交通大学出版社
http://www.bjtup.com.cn

高等学校物联网专业规划教材



网络安全概论

何小东　陈伟宏　彭智朝　**编著**

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书是作者在多次讲授研究生课程“网络与信息安全”的基础上，参考国内外相关文献，经过重新整理，编写而成的。本书概念叙述清晰，重点突出，注重知识更新和知识点的相互融合，体现了“问题驱动”和“案例教学”，每章附有实例；同时还讨论了云计算、移动互联网、物联网和大数据等新型网络技术及平台的安全性。

本书详细介绍了计算机网络安全的基本理论、相关技术和实现方法，主要内容包括：网络安全引论、密码学基础、安全认证与信息加密、网络协议的安全、网络攻防与黑客技术、网络安全扫描、恶意代码与网络病毒防治、防火墙、入侵检测系统、新型网络安全技术、网络安全系统实例、网络安全管理与风险评估等。

本书可作为高等院校计算机应用、软件工程、信息安全、电子信息及林业信息工程等专业研究生或高年级本科生相关课程教学用书，也可作为相关网络安全工程技术人员、网络安全管理人员的参考用书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13501256678　13801310933

图书在版编目(CIP)数据

网络安全概论/何小东，陈伟宏，彭智朝编著. —北京：北京交通大学出版社：清华大学出版社，2014.7
（高等学校物联网专业规划教材）
ISBN 978-7-5121-2019-8

Ⅰ. ①网… Ⅱ. ①何…②陈…③彭… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 172667 号

责任编辑：郭东青　　特邀编辑：张诗铭
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://www.bjtup.com.cn
印 刷 者：北京艺堂印刷有限公司
经　　销：全国新华书店
开　　本：185×260　　印张：21.25　　字数：530 千字
版　　次：2014 年 8 月第 1 版　　2014 年 8 月第 1 次印刷
书　　号：ISBN 978-7-5121-2019-8/TP·792
印　　数：1～2500 册　　定价：42.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。
投诉电话：010-51686043，51686008；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

随着计算机网络应用的激增，尤其是电子商务、移动互联网、物联网和各类社交网络的出现，人们的生存活动已经不只是依赖于网络，而是离不开网络了。然而，网络的安全却一直面临严峻挑战，黑客攻击、病毒传播及形形色色的网络攻击日益增加，网络安全防线脆弱，安全漏洞不断增长。在这种形势下，作者根据近几年从事计算机网络安全科研和教学的实践，编写了此书，以飨读者。

本书在编写过程中，力求做到讲清概念，突出重点，注重知识更新，把握知识点的相互融合，强调基本技术和基本应用，并在主要章节配有实例，体现问题驱动、案例教学。同时还讨论了云计算、移动互联网、物联网和大数据等新型网络及平台的安全性。本书共 14 章。每章开头有导引，列出本章的主要知识点和学习目的，每章最后有小结并附有习题，能帮助读者复习。

第 1 章对网络安全的基本概念、属性、体系结构和安全服务等进行了概括性介绍。通过本章的学习，使读者对本课程有一个初步了解，激发学习兴趣。第 2 章重点介绍了对称密钥密码和非对称密钥密码机制，具体分析了典型的对称密码算法 DES 和典型的非对称密码算法 RSA，最后简要介绍了量子密码技术。第 3 章详细介绍了认证的概念，介绍了报文认证、身份认证、接入认证和安全认证协议，讲叙了数字签名和数字摘要机制，分析了 MD5 算法，最后介绍了 CA、数字证书的组成和 PKI 协议。第 4 章主要讨论 IPSec 协议的安全问题，介绍了 IPSec 安全协议 AH、ESP 和安全联盟 SA，还讨论了 SSL 和 TSL 协议，使读者对安全协议有一个较深入的了解。第 5 章先叙述了网络攻击的分类和攻击过程，然后介绍了缓冲区溢出、拒绝服务攻击和网站的攻击与防范，最后介绍了蜜罐技术。第 6 章首先分析黑客的动机、群体和攻击流程，然后对黑客常用的攻击方法做了详细分析，并作为实例介绍了黑客对无线网络和网络设备的攻击。第 7 章介绍了防火墙的基本知识，重点介绍了包过滤、代理服务和状态检测技术，并介绍了防火墙的结构及管理的新发展；最后以 TD-W89741N 增强型防火墙为实例，介绍了防火墙的配置。第 8 章首先分析了网络产生安全漏洞的原因，重点介绍了安全扫描的原理、过程和扫描器的构成，最后作为实例介绍了一些扫描工具如：Ping 系列扫描命令、X-Scan 扫描器和 Nmap 扫描器的使用。第 9 章则介绍了入侵检测的基本概念、分类、结构和检测过程，重点介绍了入侵检测的检测技术，讲解了 IDS 系统的部署、报警策略和局限性，最后介绍了 Snort 系统和入侵检测产品等实例。第 10 章讲解了恶意代码的概念、隐藏、攻击、传播和防治机制，介绍了网络蠕虫的工作机理、检测与防治方法，使读者增强对恶意代码的认识和掌握防治软件的使用。第 11 章先介绍了信息隐藏及其检测技术，讨论了物联网、移动网及其大数据的安全问题，简介了云计算与云安全，并分析了移动互联网应用行为案例。第 12 章介绍了网络安全管理概念和安全审计，详细介绍了网络安全管理原则、评估准则、相关法律法规、灾难恢复及容灾技术等。第 13 章作为前面所学知识的综合应用

实例，详解了林业信息网络和银行信息网络安全系统的安全策略、基本架构和安全设计。

本书可作为高等院校计算机应用、软件工程、信息安全、电子信息、林业信息工程、物联网等专业研究生或高年级本科生相关课程教学使用，也可作为相关网络安全工程技术人员、网络安全管理人员的参考书。

本书由何小东、陈伟宏、彭智朝编著，何小东负责全书大纲编写及全书统稿，廖桂平负责审阅。另外，参加本书编写、插图及校对工作的还有刘军万、黄华军、李建军、陈越洲、梁小丽、彭银香、彭楚舒、何军山、刘素芝、宋霞萍、陈鹏飞、曾哲敏等。在此一并表示感谢！另北京交通大学出版社的郭东青对本书出版给予的大力支持表示感谢！

网络安全理论与技术发展迅速，编写人员水平有限，很难全面、准确地将其全貌反映出来，疏漏甚至错误之处在所难免，恳请广大读者不吝指正。

本书另配有 PPT 电子教案，有需要的老师可从出版社网站（http：//www. bjtup. com. cn）下载，或与责任编辑联系，电子邮箱：guodongqing2009@126. com。

编者

2014 年 6 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目 录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章　网络安全引论

随着计算机网络技术的发展和互联网的广泛应用，网络安全问题日益突出，已成为当今的研究焦点和社会热点而被人们所关注。那么，什么是网络安全？从广义上来讲，凡是涉及网络信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论问题都属于网络安全领域，但从本质上讲，网络安全就是指网络上的设备及信息安全。

本章将学习计算机网络安全的基本概念、体系结构、属性、内容、P2DR 模型、相关协议及标准等。主要包括以下知识点：

◇ 网络安全的概念与属性；

◇ 网络安全的内容与 P2DR 模型；

◇ 网络安全体系结构及实例；

◇ 网络安全协议；

◇ 网络安全服务。

通过本章内容的学习，读者对网络安全结构及其现状有一个较全面的了解，并且掌握网络安全的基本概念和常用的网络安全协议与服务。

1.1　概　述

计算机网络是地理上分散的多台自主计算机利用通信线路互联的集合。这些独立的计算机遵循事先约定的通信协议，通过通信设备、通信链路及网络软件实现信息交互、资源共享、协调工作及在线处理等强大功能。随着计算机网络技术的进步和互联网应用的飞速发展，确保计算机网络系统正常运行，正常存储、处理和传输数据的安全问题就显得尤为突出。

1.1.1　网络安全的概念

网络安全是指网络系统的安全运行和对在网络系统中的信息进行安全保护的统称，即网络安全包括系统运行安全和系统信息安全两个方面，它是一项动态的、整体的系统工程。从技术上来说，网络安全由安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成。

从资源上来讲，网络安全是指网络软硬件资源和信息资源的安全。硬件资源指计算机网络系统中的主机、通信设备（如：交换机、路由器等）和通信线路等硬件设施，要实现信息快速、安全地在网络中传输和交换，可靠的物理网络（硬件）部分是必不可少的。软件资源是指维持网络服务运行的各类系统软件和应用软件，而信息资源则是指在网络中存储和

传输的各种数据等。

从用户角度来看，网络安全是指保障个人数据或企业信息在网络中的保密性、完整性、不可否认性，防止信息的泄露和破坏，防止信息资源的非授权访问。而从网管角度来看，网络安全是指保障合法用户正常使用网络资源，避免计算机病毒、拒绝服务、远程控制、非授权访问等安全威胁，及时发现安全漏洞，制止攻击行为。

综上所述，网络安全是指保护网络系统中的软硬件资源及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络系统正常运行、网络服务不中断。这也是网络安全的一个通用定义。

1.1.2 网络安全的属性

所谓网络安全的属性，是指网络系统的可用性（availability）、可控性（controllability）、完整性（integrity）、机密性（confidentiality）和不可抵赖性（non-repudiation）这五个方面的性能，一个网络系统只有具备这五个方面的属性，才能说是安全的。

1. 可用性（availability）

所谓可用性是指网络系统能保证信息和系统不间断地为授权者提供服务，而不会出现非授权者滥用和对授权者拒绝或中断服务的情况。这在许多银行、企业等客服网络系统中非常重要，系统服务往往每天 24 小时不能中断。

2. 可控性（controllability）

所谓可控性是指网络系统能始终被合法管理者所有效、安全地监控和管理，防止被非法利用。如：网络系统中的服务器就必须被管理员所控制，而不能被非法者所控制。

3. 完整性（integrity）

所谓完整性是指网络系统保证信息从真实的发送者通过网络传送到真实的接收者手中，网络传送过程中没有被他人添加、删除、修改和替换，信息是真实和完整的。

4. 机密性（confidentiality）

所谓机密性是指网络系统保证信息为授权者享用，而不泄漏给未经授权者。

5. 不可抵赖性（non-repudiation）

所谓不可抵赖性是指信息的行为人要为自己的行为负责，提供保证社会依法管理需要的公证、仲裁信息证据。不可抵赖性又称不可否认性，在一些商业活动（如：电子商务）中尤为重要。

1.1.3 网络安全的内容

网络安全的内容包括：物理安全、安全控制、安全服务和安全机制等。

1. 物理安全

指自然灾难（如：雷电、地震、火灾等）、物理损坏（如：硬盘损坏、设备使用寿命到期等）、设备故障（如：停电、电磁干扰等）、意外事故等。另外，物理安全还包括：电磁泄漏、信息泄漏、操纵失误、意外疏漏等。

2. 安全控制

安全控制包括操纵系统、网络接口模块和网络互联设备的安全控制。如用户开机输入的口令（某些微机主板有“万能口令”），对文件的读写存取的控制（如：UNIX 系统的文件属

性控制机制）。安全控制主要用于保护存储在硬盘上的信息和数据。另外，在网络环境下要对来自其他机器的网络通信进程进行安全控制。包括：身份认证、客户权限设置与判别、审计日志等。另外，通过网管软件或路由器配置，对整个子网内的所有主机的传输信息和运行状态，进行安全监测和控制。

3. 安全服务

现行计算机网络系统提供包括：实体认证服务、访问控制服务、数据保密服务、数据完整性服务和不可否认服务等在内的多种安全服务。有关这些安全服务的具体内容将在后面加以介绍。

4. 安全机制

计算机网络系统实施包括：加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、信息流填充机制、路由控制机制和公证机制等在内的多种安全机制。有关这些安全机制的具体内容将陆续在后面章节进行介绍。

1.1.4　网络安全模型

网络安全是指系统的安全，需要构建一个理论上的框架，这个框架就是网络安全模型。所谓安全模型是指在整体安全策略的控制和指导下，在综合运用防护工具（如：防火墙、操作系统身份认证、加密等手段）的同时，利用检测工具（如：漏洞评估、入侵检测等系统）了解和评估系统的安全状况，将系统调整到“最安全”和“风险最低”的状态。目前最常用的网络安全模型是 P2DR 模型，即 Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）模型。这是一个完整的、动态的安全循环模型，在安全策略的指导下，保证网络系统的安全。

按照 P2DR 模型，安全策略是整个网络安全的依据，不同的网络需要不同的安全策略。在制定策略以前需要全面考虑，如局域网如何在网络层实现安全性？如何控制远程用户的访问？在广域网上的数据传输如何实现安全加密传输？以及如何进行用户的认证等问题。对这些问题做出详细回答，并确定相应的防护手段和实施办法，就是一份完整的网络安全策略，策略一旦制定，应作为整个网络安全行为的准则。

P2DR 模型是基于时间的一种安全理论（Time Based Security），它认为：与信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为还是响应行为都要消耗时间，因此可以用时间来衡量一个体系的安全性和安全能力。攻击成功花费的时间就是安全体系提供的防护时间，设为 P_t；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间，即检测时间，设为 D_t；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间，即响应时间，设为 R_t。

于是，P2DR 模型用数学公式表示为：

$$P_t > D_t + R_t \tag{1}$$

式中：P_t——系统为了保护安全目标，设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所花费的时间；

D_t——从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间；

R_t——从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。

针对需要保护的安全目标，当上述数学公式满足防护时间大于检测时间加上响应时间时，也就是在入侵者危害安全目标之前，就能够被检测到并及时得到处理。假设防护时间 $P_t=0$，那么：

$$D_t+R_t=E_t \tag{2}$$

式中：D_t——从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间；R_t——从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。如：对 Web Server 被破坏的页面进行恢复。

E_t——D_t 与 R_t 之和，也就是该安全目标系统的暴露时间。针对需要保护的安全目标，如果 E_t 越小，表明系统越安全。

通过上面两个公式的描述，可以得到“安全”的定义。即：“及时的检测和响应就是安全”或“及时的检测和恢复就是安全”。该定义给出了解决安全问题的方法，即提高系统的防护时间 P_t，降低检测时间 D_t 和响应时间 R_t。当然，在实际当中，安全不能依靠单纯的静态防护，也不能依靠单纯的技术来解决，还需要动态的技术和规范的管理。未来的网络安全理论和管理呈现出以下发展趋势。

1. 高度灵活和自动化的网络安全管理

网络安全的管理更加灵活和自动化，人们借助相关辅助工具管理相当庞大的网络；通过对安全数据进行自动的多维分析和汇总，使人们从海量的安全数据中解脱出来；根据所提交的决策报告，进行安全策略的制定和安全决策。

2. 安全管理与网络管理集成

由于网络安全问题的复杂性，网络安全管理将与已经较成熟的网络管理集成，在统一的平台上实现网络管理和安全管理。

3. 检测技术更加细化

将产生针对各种新的应用程序漏洞的评估和入侵监控技术及新的攻击追踪技术等，这些技术将逐步应用到网络安全管理的各个环节中。

总之，以 P2DR 模型为主导的安全理论，将随着技术的发展而不断得到完善。

1.2 网络安全体系结构

网络安全体系结构是对网络安全的抽象描述，是从系统的角度理解网络安全问题，对研究、实现和管理网络安全具有全局性的指导作用。网络安全体系结构可描述为：①为满足用户需求而必须提供的一套安全服务；②要求所有系统元素都要实现的服务；③为应对环境威胁而要求系统元素达到的安全级别。在学习网络安全体系结构知识之前，应先了解什么是计算机网络体系结构。本节将讲述网络安全体系结构的基本概念和内容，并以 OSI 和 TCP/IP 两种常用的网络安全体系结构为实例，最后介绍部分网络安全协议和标准。

1.2.1 网络分层体系结构

网络安全体系结构应包括：管理安全、通信安全、计算机安全、网络安全、人员安全和物理安全等。它既需要对付恶意威胁，也要对付意外的威胁。计算机网络体系结构从功能的

此为试读，需要完整PDF请访问：www.ertongbook.com