21世纪高等院校规划教材

网络信息安全技术

THE NETWORK INFORMATION SECURITY TECHNOLOGY

刘永华　主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

21 世纪高等院校规划教材

网络信息安全技术

刘永华　主编

王公堂　孙俊香　陈　茜　张淑玉　刘　芳　副主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书的内容涵盖了网络安全和管理的基本概念、原理和技术。全书共分8章，主要内容包括网络安全概述、操作系统安全、数据库与数据安全、数字加密与认证、防火墙技术、入侵监测技术、网络病毒的防治、网络维护等内容。本书内容全面，取材新颖，既有网络安全和管理的理论知识，又有实用技术，反映了网络安全和管理技术的最新发展状况。

本书适合作为普通高等院校计算机科学与技术、网络工程、通信工程、自动化及相关专业本科教材，也可作为成人高等教育计算机网络安全教材，还可作为广大工程技术人员的科技参考书。

图书在版编目（CIP）数据

网络信息安全技术/刘永华主编. —北京：中国铁道出版社，2011.7

21世纪高等院校规划教材

ISBN 978-7-113-12926-2

Ⅰ.①网… Ⅱ.①刘… 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（2011）第081354号

书　　名：网络信息安全技术
作　　者：刘永华　主编

策划编辑：杨　勇
责任编辑：秦绪好　　**读者热线：**400-668-0820
编辑助理：何　佳　　**封面设计：**付　巍
责任印制：李　佳　　**封面制作：**白　雪

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京新魏印刷厂
版　　次：2011年7月第1版　　2011年7月第1次印刷
开　　本：787mm×1092mm　1/16　**印张：**16.5　**字数：**371千
印　　数：3 000册
书　　号：ISBN 978-7-113-12926-2
定　　价：28.00元

前言

FOREWORD

在全球信息化的背景下，信息已成为一种重要的战略资源。信息的应用涵盖国防、政治、经济、科技、文化等各个领域，在社会生产和生活中的作用愈来愈显著。随着 Internet 在全球的普及和发展，计算机网络成为信息的主要载体之一。网络信息技术的应用愈加普及和广泛，应用层次逐步深入，应用范围不断扩大。国家发展和社会运转、计算机网络的全球互联趋势，都显现出人类活动对计算机网络的依赖性不断增大，这也使得网络安全问题更加突出，并受到越来越广泛的关注。计算机网络的安全性已成为当今信息化建设的核心问题之一。

网络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，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。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。全书共分 8 章，内容安排如下：

第 1 章　具体介绍计算机网络安全的相关基础知识，包括网络安全的概念及影响网络安全的主要因素、网络安全威胁以及网络安全常用的技术。

第 2 章　主要介绍操作系统安全技术，包括 Windows 和 Linux 操作系统的安全机制、安全漏洞和安全配置方案。

第 3 章　介绍数据库与数据安全技术，包括数据库的安全特性、数据库的安全保护、数据的完整性、数据备份和恢复、网络备份、系统数据容灾等。

第 4 章　介绍网络安全中的密码技术，包括传统的加密方法、数据加密标准、公开密钥算法和数字签名等技术。

第 5 章　介绍访问控制技术中的防火墙技术，包括防火墙的原理、种类和实现策略等。

第 6 章　主要对入侵检测的概念和相关技术进行了全面介绍，并对入侵检测的未来发展进行了讨论。

第 7 章　主要介绍病毒的原理、病毒的类型和计算机网络病毒，同时介绍几种影响较大的网络病毒，如 CIH 病毒、Word 宏病毒、蠕虫病毒和木马病毒等，并且介绍了病毒的清除及防护措施。

第 8 章　主要介绍 Windows 自带的常用网络工具，讨论了网卡、集线器、交换机、路由器、网线和 RJ-45 接头等网络连接设备的维护、网络性能优化等问题，重点介绍常用网络故障及排除方法。

由于网络安全的内容非常丰富，本书按理论教学以“必需、够用”为度，加强实践性环节教学，提高学生实际技能的原则组织编写。全书讲究知识性、系统性、条理性、

连贯性；力求激发学生兴趣，注重提示各知识点之间的内在联系，精心组织内容，做到由浅入深，由易到难，删繁就简，突出重点；适于课堂教学和实践教学。

通过对本书的学习，可使读者较全面地了解网络系统安全的基本概念、网络安全技术和应用，培养读者解决网络安全问题的能力。本书共 8 章，适用于 48 学时左右的课堂教学。

本书适合作为普通高等院校计算机科学与技术、网络工程、通信工程、自动化及相关专业本科教材，也可作为成人高等教育计算机网络安全教材，还可作为广大工程技术人员的科技参考书。

本书由刘永华担任主编并统稿，王公堂、孙俊香、陈茜、张淑玉、刘芳担任副主编。其中刘永华完成了第 3、4、5 章的编写，王公堂完成了第 2 章的编写，孙俊香完成了第 6 章的编写、陈茜完成了第 7 章的编写，张淑玉完成了第 1 章的编写，刘芳完成了第 8 章的编写。赵艳杰、王梅、于春花、李晓利、解圣庆参与了本书的讨论，并提了许多宝贵意见，在此向他们表示感谢。

由于作者水平有限，加之编写时间仓促，书中难免存在疏漏与不足之处，恳请广大读者和同行批评指正。

编　者

2011 年 4 月

CONTENTS

目 录

第 1 章 网络安全概述

学习目标

系统学习网络安全的概念，网络面临的主要威胁，影响网络安全的因素，保证网络安全的技术。通过学习本章，读者应掌握和了解以下内容：

- 掌握：网络安全的概念，网络安全的基本技术。
- 了解：网络的安全威胁，影响网络安全的主要因素。

随着信息技术的迅速发展，网络已成为全球重要的信息传播工具。而随着互联网的飞速发展，网络安全问题已经越来越受到人们的关注，各种病毒花样繁多、层出不穷；系统、程序、软件的安全漏洞越来越多；黑客通过不正当手段侵入他人计算机，非法获得信息资料，给正常使用互联网的用户带来不可估量的损失。因此，网络安全越来越引起人们的重视。

1.1 网络安全简介

20 世纪 90 年代中期以来，随着网络技术突飞猛进的发展，特别是 Internet 的迅猛发展，各国的信息化进程急剧加快。我国的信息化热潮也随之高涨，信息应用也从原来的军事、科技、文化和商业渗透到社会生活的各个领域，在社会生产、生活中的作用日益显著。人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密问题。网络信息安全技术经过十几年的发展，在信息安全技术的研究上形成了两个完全不同的角度和方向：一个从正面防御考虑，研究加密、鉴别、认证、授权和访问控制等；另一个从反面攻击考虑，研究漏洞扫描评估、入侵检测、紧急响应和防病毒。

1.1.1 网络安全的概念

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。下面给出网络安全的一个通用定义：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，系统能连续可靠正常地运行，网络服务不中断。

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。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两者相互补充，缺一不

可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。

网络安全要考虑以下几个方面的内容。

1. 网络系统的安全

主要包括以下几方面的问题：

- 网络操作系统的安全性：目前流行的操作系统（UNIX、Windows 2000/ NT/XP/T 等）均存在网络安全漏洞。
- 来自外部的安全威胁。
- 来自内部用户的安全威胁。
- 通信协议软件本身缺乏安全性（如 TCP/IP）。
- 计算机病毒感染。
- 应用服务的安全：许多应用服务系统在访问控制及安全通信方面考虑得不周全。

2. 局域网安全

局域网采用广播方式，在同一个广播域中可以侦听到在该局域网上传输的所有信息包，这是一个不安全的因素。

3. Internet 互联安全

非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒等都是在 Internet 上经常遇到的问题。

4. 数据安全

事实上，无论 Internet 还是其他专用网络，都必须注意数据的安全性问题，以保护本单位、本部门的信息资源不会受到外来的侵害。

从根本意义上讲，绝对安全的计算机是根本不存在的，绝对安全的网络也是不可能有的。只有存放在一个无人知晓的密室里，而又不插电的计算机才可以称之为安全。计算机只要投入使用，就或多或少地存在着安全问题，只是程度不同而已。因此，在探讨网络安全的时候，实际上指的是一定程度的网络安全。而到底需要多大的安全性，要依据实际需要及自身能力而定。网络安全性越高，同时也意味着网络的管理越复杂。网络的安全性与网络管理便利性是相互矛盾的。

1.1.2 网络安全模型

典型的网络安全模型如图 1-1 所示。信息需要从一方通过网络传送到另一方。在传送中居主体地位的双方必须合作以便进行交换。通过通信协议（如 TCP/IP）在两个主体之间可以建立一条逻辑信息通道。

为防止对手对信息机密性、可靠性等造成破坏，需要保护传送的信息。保证安全性的所有机制包括以下两部分：

- 对被传送的信息进行与安全相关的转换。图 1-1 中包含了消息的加密和以消息内容为基础的补充代码。加密消息使对手无法阅读，补充代码可以用来验证发送方的身份。
- 两个主体共享不希望对手得知的保密信息。例如，使用密钥链接，在发送前对信息进行转换，在接收后再转换回来。

为了实现安全传送，可能需要可信任的第三方。例如，第三方可能会负责向两个主体分发保密信息，而向其他对手保密，或者需要第三方对两个主体间传送信息可靠性的争端进行仲裁。

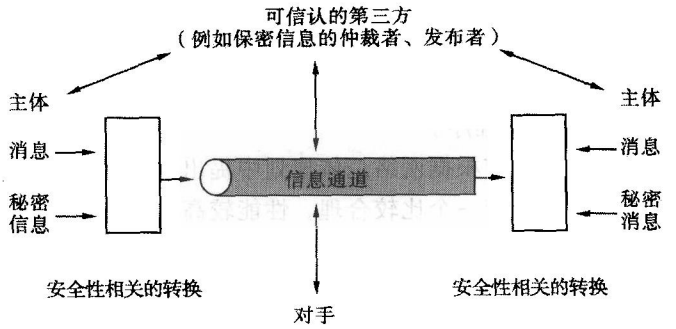

图 1-1　网络安全模型

这种通用模型指出了设计特定安全服务的 4 个基本任务。

- 设计执行与安全性相关的转换算法，该算法必须使对手不能对算法进行破解以实现其目的。
- 生成算法使用的保密信息。
- 开发分发和共享保密信息的方法。
- 指定两个主体要使用的协议，并利用安全算法和保密信息来实现特定的安全服务。

1.1.3　计算机安全的分级

计算机操作系统的安全级别在美国国防部发表的橘皮书——《可信计算机系统评测标准》中，把计算机系统分为 4 个等级、7 个级别，即 D（最低保护等级）、C（自主保护等级）、B（强制保护等级）、A（验证保护等级）四等，细分为 D1、C1、C2、B1、B2、B3、A1 七级。

- D1 级：计算机安全的最低一级，不要求用户进行登录和密码保护，任何人都可以使用，整个系统是不可信任的，硬件和软件都易被侵袭。
- C1 级：自主安全保护级。要求硬件有一定的安全级（如计算机带锁），用户必须通过登录认证方可使用系统，并建立了访问许可权限机制。
- C2 级：受控存取保护级。比 C1 级增加了几个特性——引进了受控访问环境，进一步限制了用户执行某些系统指令；授权分级使系统管理员给用户分组，授予他们访问某些程序和分级目录的权限；采用系统审计，跟踪记录所有安全事件及系统管理员的工作。
- B1 级：标记安全保护级。对网络上每个对象都给予实施保护；支持多级安全，对网络、应用程序工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。
- B2 级：结构化保护级。对网络和计算机系统中所有对象都加以定义，给一个标签；为工作站、终端等设备分配不同的安全级别；按最小特权原则取消权力无限大的特权用户。
- B3 级：安全域级。要求用户工作站或终端必须通过可信任的途径链接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，

将系统管理员、系统操作员和系统安全员的职责分离，将人为因素对计算机安全的威胁降至最小。

- A1 级：验证设计级。这是计算机安全级中最高的一级，本级包括了以上各级别的所有措施，并附加了一个安全系统的受监视设计；合格的个体必须经过分析并通过这一设计；所有构成系统的部件的来源都必须有安全保证；这一级还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

在网络的具体设计过程中，应根据网络总体规划中提出的各项技术规范、设备类型、性能要求以及经费等，综合考虑来确定一个比较合理、性能较高的网络安全级别，从而实现网络的安全性和可靠性。

1.1.4 网络安全的重要性

在信息社会中，信息具有与能源、物源同等的价值，在某些时候甚至具有更高的价值。具有价值的信息必然存在安全性的问题，对于企业更是如此。例如，在竞争激烈的市场经济驱动下，每个企业对于原料配额、生产技术、经营决策等信息，在特定的地点和业务范围内都具有保密的要求，一旦这些机密被泄露，不仅会给企业，甚至也会给国家造成严重的经济损失。

经济社会的发展要求各用户之间进行通信和资源共享，需要将一批计算机连成网络，这样就隐含着很大的风险，包含了极大的脆弱性和复杂性，特别是当今最大的网络——Internet，很容易遭到别有用心者的恶意攻击和破坏。随着国民经济信息化程度的提高，有关的大量情报和商务信息都高度集中地存放在计算机中。随着网络应用范围的扩大，信息的泄露问题也变得日益严重，因此，计算机网络的安全性问题就越来越重要。

1.2 网络安全现状

互联网与生俱来的开放性、交互性和分散性特征使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨大推动力。正是由于互联网的上述特性，产生了许多安全问题：

- 黑客（英文 Hacker 的译音）入侵。黑客是指在 Internet 上的一批熟悉网络技术的人，他们经常利用网络上现存的一些漏洞，设法进入他人的计算机系统。有些人只是为了好奇，而有些人是存在不良动机侵入他人系统，他们偷窥机密信息，或将其计算机系统破坏，这部分人都被称为“黑客”。攻击、计算机病毒破坏和网络金融犯罪已构成对世界各国的实际威胁。进入 21 世纪以来，尽管人们在计算机技术上做出了种种努力，但这种攻击却是愈演愈烈。从单一地利用计算机病毒搞破坏和用黑客手段进行入侵攻击转变为使用恶意代码与黑客攻击手段相结合的方式，使得这种攻击具有传播速度惊人、受害面惊人和穿透深度广的特点，往往一次攻击就会给受害者带来严重的破坏和损失。
- 信息泄露、信息污染、信息不易受控。例如，资源未授权侵用、未授权信息流出现、系统拒绝信息流和系统否认等，这些都是信息安全的技术难点。
- 在网络环境中，一些组织或个人出于某种特殊目的，进行信息泄密、信息破坏、信息侵

权和意识形态的信息渗透，甚至通过网络进行政治颠覆等活动，使国家利益、社会公共利益和各类主体的合法权益受到威胁。

- 网络运用的趋势是全社会广泛参与，随之而来的是控制权分散的管理问题。由于人们的利益、目标、价值的分歧，使信息资源的保护和管理出现脱节和真空，从而使信息安全问题变得广泛而复杂。
- 随着社会重要基础设施的高度信息化，社会的“命脉”和核心控制系统有可能面临恶意攻击而导致损坏和瘫痪，包括国防通信设施、动力控制网、金融系统和政府网站等。

近年来，人们的网络安全意识逐步提高，很多企业根据核心数据库和系统运营的需要，逐步部署了防火墙、防病毒和入侵监测系统等安全产品，并配备了相应的安全策略。虽然有了这些措施，但并不能解决一切问题。我国网络安全问题日益突出，其主要表现为以下几个方面。

1．安全事件不能及时准确发现

网络设备、安全设备、系统每天生成的日志可能有上万甚至几十万条，这样人工地对多个安全系统的大量日志进行实时审计、分析流于形式，再加上误报（典型的如 NIDS、IPS）、漏报（如未知病毒、未知网络攻击、未知系统攻击）等问题，造成不能及时准确地发现安全事件。

2．安全事件不能准确定位

信息安全系统通常是由防火墙、入侵检测、漏洞扫描、安全审计、防病毒、流量监控等产品组成的，但是由于安全产品来自不同的厂商，没有统一的标准，所以安全产品之间无法进行信息交流，于是形成许多安全孤岛和安全盲区。由于事件孤立，相互之间无法形成很好的集成关联，因而一个事件的出现不能关联到真实问题。

如入侵监测系统事件报警，就须关联同一时间防火墙报警、被攻击的服务器安全日志报警等，从而了解是真实报警还是误报；如是未知病毒的攻击，则分为两类：网络病毒、主机病毒。网络病毒大都表现为流量异常，主机病毒大都表现为中央处理器异常、内存异常、磁盘空间异常、文件的属性和大小改变等。要发现这个问题，需要关联流量监控（网络病毒）、关联服务器运行状态监控（主机病毒）、关联完整性检测（主机病毒）来发现。为了预防网络病毒大规模爆发，必须在病毒爆发前快速发现中毒机器并切断源头。如服务器的攻击，可能是安全事件遭病毒感染；DDoS 攻击，可能是服务器 CPU 超负荷；端口某服务流量太大、访问量太大……，必须将多种因素结合起来才能更好地分析，快速了解真实问题点并及时恢复正常。

DDoS（Distributed Denial of Service，分布式拒绝服务）是一种基于 DoS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，如商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

3．无法做集中的事件自动统计

某台服务器的安全情况报表、所有机房发生攻击事件的频率报表、网络中利用次数最多的攻击方式报表、发生攻击事件的网段报表、服务器性能利用率最低的服务器列表等。需要管理员人为地对这些事件做统计记录，生成报告，从而耗费大量人力。

4．缺乏有效的事件处理查询

没有对事件处理的整个过程做跟踪记录，信息部门主管不了解哪些管理员对该事件进行了处理，处理过程和结果也没有做记录，使得处理的知识经验不能得到共享，导致下次再发生类似事件时，处理效率降低。

5．缺乏专业的安全技能

管理员发现问题后，往往因为安全知识的不足导致事件迟迟不能被处理，从而影响网络的安全性、延误网络的正常使用。

1.3 网络安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。

安全威胁可分为故意的（如黑客渗透）和偶然的（如信息被发往错误的地址）两类。故意威胁又可进一步分为被动和主动两类。

1.3.1 网络安全攻击

对于计算机或网络安全性的攻击，一般是通过在提供信息时查看计算机系统的功能来记录其特性。当信息从信源向信宿流动时，图 1-2 列出了信息正常流动和受到各种类型的攻击的情况。

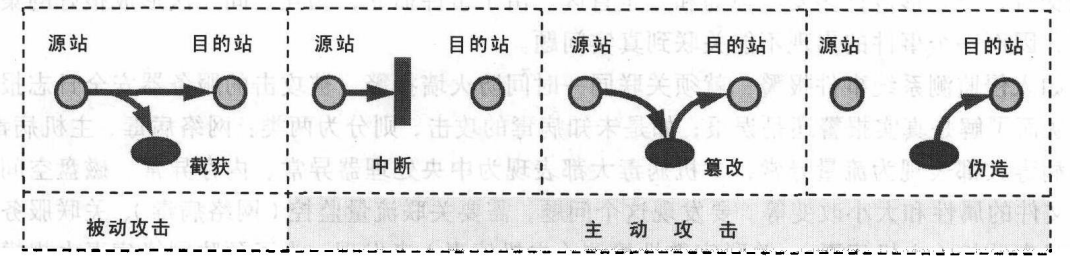

图 1-2 安全攻击

- 中断是指系统资源遭到破坏或变得不能使用。这是对可用性的攻击。例如，对一些硬件进行破坏、切断通信线路或禁用文件管理系统。
- 截获是指未授权的实体得到了资源的访问权，这是对保密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。例如，为了捕获网络数据的窃听行为，以及在未授权的情况下复制文件或程序的行为。
- 篡改是指未授权的实体不仅得到了访问权，而且还修改了资源，这是对完整性的攻击。例如，在数据文件中改变数值、改动程序使它按不同的方式运行、修改在网络中传送的信息的内容等。
- 伪造是指未授权的实体向系统中插入捏造的对象，这是对真实性的攻击。例如，向网络中插入欺骗性的消息，或者向文件中插入额外的记录。

这些攻击可分为被动攻击和主动攻击两种。