普通高等教育“十三五”规划教材
高等院校计算机系列教材

网络安全与密码技术导论

李 浪 欧阳陈华 厉阳春◉主编

華中科技大學出版社
http://www.hustp.com

普通高等教育“十三五”规划教材
高等院校计算机系列教材

网络安全与密码技术导论

主　编　李　浪　欧阳陈华　厉阳春
副主编　李仲生　谢新华　许琼方

华中科技大学出版社
中国·武汉

内 容 简 介

本书是结合多年教学和实践经验、参考国内外有关著作而编写的一本关于网络安全与密码技术的实用教程。本书内容涵盖了网络安全与密码技术的基本概念、原理和技术，目的是使学习者通过学习，能够掌握密码技术的基本原理、密码算法的构成和加、解密过程，熟悉网络安全的技术原理和常用网络安全软件的使用方法。

本书内容详实、重点难点突出，所选案例具有较强的代表性，有助于学习者举一反三。全书注重理论性和实用性的结合，特别适合作为高等院校、各类职业院校及计算机培训学校相关专业的课程教材，也可作为广大网络工程技术人员的科技参考用书。

图书在版编目(CIP)数据

网络安全与密码技术导论/李浪，欧阳陈华，厉阳春主编. —武汉：华中科技大学出版社，2015.7
ISBN 978-7-5680-1110-5

Ⅰ.①网… Ⅱ.①李… ②欧阳… ③厉… Ⅲ.①计算机网络-安全技术 ②计算机网络-密码术
Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 179487 号

网络安全与密码技术导论 李 浪 欧阳陈华 厉阳春 主编

策划编辑：朱建丽 范 莹
责任编辑：谢 婧
封面设计：原色设计
责任校对：张 琳
责任监印：周治超
出版发行：华中科技大学出版社(中国·武汉)
武昌喻家山 邮编：430074 电话：(027)81321913
录 排：武汉楚海文化传播有限公司
印 刷：武汉市籍缘印刷厂
开 本：787mm×1092mm 1/16
印 张：17
字 数：414 千字
版 次：2015 年 9 月第 1 版第 1 次印刷
定 价：39.80 元

前　言

在全球信息网络化背景下，网络已经成为一种国家级的战略资源。随着人类活动对计算机网络的依赖性不断增大，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破坏、更改、泄露，系统连续可靠运行，网络服务不中断。网络安全的首要特性即保密性，它的核心技术就是密码技术，其目的是实现隐秘地传递信息。

由于网络安全和密码技术的内容非常丰富，本书按照理论教学以“必需、够用”为度，加强实践教学环节，提高学生实践动手能力的原则组织编写。全书讲究知识性、系统性、条理性、连贯性，力求激发学生学习兴趣，注重理顺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，适合课堂教学和实践教学。

全书共分 11 章，第 1 章介绍了信息与网络安全的概念、面临的威胁、常用的网络安全管理技术和我国的信息安全管理标准和措施；第 2 章对加密技术（主要是加密算法）进行了详细的描述，介绍了一些安全认证和密码破译的方法；第 3 章主要介绍了当前几种常见的网络攻击方式和防范方法；第 4 章主要介绍了网络防火墙的概念、作用、技术和体系结构；第 5 章介绍了入侵检测系统的类型与技术，以及入侵检测技术的实施和发展方向；第 6 章讲述了计算机病毒的概念、产生和发展，以及计算机病毒的特征和传播途径，简要介绍了计算机病毒的破坏行为以及如何防御计算机病毒和查杀计算机病毒；第 7 章介绍了无线网络安全的基础知识，以及无线网络面临的安全威胁，从无线局域网、无线城域网、无线广域网三个不同的角度描绘了无线网络安全的解决方案；第 8 章介绍了 VPN 的有关知识，并详细地论述了 Windows2003 下的 VPN 服务器配置过程和在 Win7 下登录 VPN 的设置过程；第 9 章针对当前严峻的网络安全形势，从 4 种常见网络行为出发，介绍了相应的安全防范措施；第 10 章介绍了大数据环境下的云计算安全和移动支付安全；第 11 章介绍了软件保护的相关知识。每个章节均配有习题和教学课件。

本书由李浪、欧阳陈华、厉阳春担任主编并统稿，李仲生、谢新华、许琼方担任副主编。其中第 1、2 章由厉阳春编写，第 3、8、10 章由欧阳陈华编写，第 4、6、9 章由谢新华编写，第 5、7、11 章由许琼方编写。李浪对全书的架构进行了设计，并对全书进行了多次审校与修改，李仲生对目录与章节安排提出了指导性意见，并参与了部分内容的编写。本书的作者都是多年从事网络安全教学和密码学研究的大学教师，在编写的过程中，参考了国内外大量文献资料，结合了多年教学科研经验及成果。尽管我们再三校对，书中可能还存在错误和不

足，恳请广大专家和读者指正和谅解。

本书不仅可以作为高等院校、各类职业院校及计算机培训学校相关专业的课程教材，还可作为网络工程技术人员的科技参考用书。同时，本书已开发好相应的教学 PPT 课件，有需要的老师可以在华中科技大学出版社的网页上下载，也可发邮件向我们索取，我们的邮箱是 lilang911@126.com。

编　者

2015 年 5 月

目　录

第1章　信息安全概述

1.1　信息与网络安全概念

1.1.1　互联网的发展

20世纪70年代末到80年代初，计算机网络蓬勃发展，各种各样的计算机网络应运而生，网络的规模和数量都得到了很大的发展。一系列网络的建设，产生了不同网络之间互联的需求，并最终导致了TCP/IP协议的诞生。1980年，TCP/IP协议研制成功。1982年，ARPNET开始采用IP协议。1986年美国国家科学基金会NSF资助建成了基于TCP/IP技术的主干网NSFNET，用于连接美国的若干超级计算中心、主要大学和研究机构，世界上第一个互联网产生，迅速连接到世界各地。20世纪90年代，随着Web技术和相应浏览器的出现，互联网的发展和应用出现了新的飞跃。1995年，NSFNET开始商业化运行。1994年4月20日，中国科学院计算机网络信息中心NCFC工程通过美国Sprint公司连入Internet的64KB国际专线开通，实现了与Internet的全功能连接。从此中国被国际上正式承认为拥有全功能Internet的国家。

1995年以来，互联网用户数量呈指数增长趋势，平均每半年翻一番。截止到2013年6月，全球已经有超过22亿用户，其中中国网民数达5.91亿，网络普及率达44.41%，手机网民数达4.64亿。随着物联网技术的发展和4G手机的普及，网民数量仍将以较高的速度增长。

1.1.2　计算机、网络、信息的关系

网络用来传输信息、交换信息，计算机用来处理信息、存储信息。没有计算机，网络难以完成传输信息、交换信息的任务。同样，没有网络，计算机就不能充分发挥处理信息、存储信息的作用。若没有计算机和网络，海量的信息就无法传输、处理、存储，我们这个时代也就不能称为信息时代。21世纪，计算机、网络和信息这三个概念已变得相辅相成、不可分割，探讨和研究三者中的任何一个问题，都离不开另外两者。计算机和网络的问世和发展，是人类社会和科技进步的结果，最终落脚点是信息，因此，信息安全是我们的根本目标，但其离不开计算机和网络的安全。

1.1.3　计算机网络安全的定义

由于网络的定义有多种，所以各种关于网络与信息安全的定义也不同。有的定义说，网络安全就是保护网上保存和传输的数据不被他人偷看、窃取或修改。也有的定义为，信息安全是指保护信息财产，以防止偶然或未被授权者对信息的泄露、修改和破坏，从而导致信息的不可信或无法处理。综合来看，计算机网络安全是指利用网络管理控制和技术措施，保证

在一个网络环境里信息数据的保密性、完整性及可使用性受到保护。网络安全的主要目标是要确保经网络传送的信息，在到达目的站时没有任何增加、改变、丢失或被非法读取。具体来讲，网络安全包括以下 5 个基本要素。

(1) 机密性。确保信息不暴露给未经授权的人或应用进程。

(2) 完整性。只有得到允许的人或应用进程才能修改数据，并且能够判别出数据是否被更改。

(3) 可用性。只有得到授权的用户在需要时才可以访问数据，即使在网络被攻击时也不能阻碍授权用户对网络的使用。

(4) 可控性。能够对授权范围内的信息流向和行为方式进行控制。

(5) 可审查性(也称为不可抵赖性)。当网络出现安全问题时，能够提供调查的依据和手段，保证用户在事后无法否认曾经对信息进行的生成、签发、接收等行为。

1.2 信息安全的重要性与所面临的威胁

1.2.1 信息安全的重要性

1946 年，世界上第一台电子计算机在美国诞生后，经过 60 多年的发展，作为社会发展三要素的物质、能源和信息的关系发生了深刻的变化。在计算机技术和通信技术的推动下，信息要素已成为支配人类社会发展进程的决定性力量之一，信息关系到一个人的成长、一个单位的业务发展，甚至一个国家的生死存亡。可以这么说，我们的社会已经开始从工业化社会进入到信息化社会。

微型计算机和大容量存储技术的发展和应用，推动了信息处理的电子化；通信技术和通信协议的发展推动了信息的高速传输和信息资源的广泛共享。20 世纪 80 年代以后，特别是 20 世纪 90 年代中后期开始的互联网狂潮，彻底改变了人们获取知识、了解信息的习惯，互联网已经成为继电视、电台、报刊之后的第四大媒体，是我们获取信息、传播信息的重要载体。互联网的使用已经深入到政治、军事、文化、商务、学习和日常生活等各个领域和方面，深刻影响着社会各阶层、个人、政体，甚至国家内部及相互之间关系的思维方式、行为方式和观念的变化。

1. 社会信息化提升了信息的地位

在国民经济和社会各个领域，不断推广和应用计算机、通信、网络等信息技术和其他相关智能技术，达到全面提高经济运行效率、劳动生产率、企业核心竞争力和人民生活质量的目的。信息化是工业社会向信息社会的动态发展过程。在这一过程中，信息产业在国民经济中所占比例上升，工业化与信息化的结合日益密切，信息资源成为重要的生产要素。

2. 社会对信息技术的依赖性增强

信息化已经成为当今世界经济和社会发展的趋势，这种趋势主要表现在：信息技术突飞猛进，成为新技术革命的领头羊；信息产业高速发展，成为经济发展的强大推动力；信息网络迅速崛起，成为社会和经济活动的重要依托。

网络应用已从简单获取信息发展为进行学习、学术研究、休闲娱乐、情感交流、社交、获得各种免费资源、对外通信和联络、网上金融、网上购物、商务活动、追崇时尚等多元化应用。

3. 虚拟的网络财富日益增长

互联网的普及，使得财产的概念除金钱、实物外，又增加了虚拟的网络财富，网络账号、各种游戏装备、游戏积分、游戏币等都是人们的财产体现，而这些虚拟财产都以信息的形式在网络中流通并使用，网络信息安全直接关系到这些财产的安全，同时，这种形式的财产保护也对我们现今的法律提出了新的要求。

4. 信息安全已经成为社会的焦点问题

信息使用比例的增大，使得社会对信息的真实程度、保密程度和要求不断提高，而网络化又使因虚假、泄密引起的信息危害程度越来越大。如近几年的大学英语四、六级考题泄漏事件，通过网络操作的股民账户受损事件，“熊猫烧香”病毒导致计算机网络大面积瘫痪等影响都是全国性的；2013年美国“棱镜”事件导致美国不仅与对立国家，甚至与传统盟国之间都产生了严重的隔阂。

1.2.2　信息安全所面临的威胁

威胁定义为对缺陷的潜在利用，这些缺陷可能导致非授权访问、信息泄漏、资源耗尽、资源被盗或者被破坏等。信息安全所面临的威胁可能来自很多方面，并且是随着时间的变化而变化的。一般而言，主要的威胁种类有如下几种。

(1) 窃听。在广播式网络信息系统中，每个节点都能读取网上传输的数据。对广播网络的双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得黑客等很容易窃取网上的数据或非授权访问且不易被发现。

(2) 假冒。当一个实体假扮成另一个实体时就发生了假冒。一个非授权节点，或一个不被信任的、有危险的授权节点都能冒充一个完全合法的授权节点，而且冒充难度不大。很多网络适配器都允许网络数据帧的源地址由节点自己来选取或改变，这就使冒充变得较为容易。

(3) 重放。重放是攻击方重新发送一份合法报文或报文的一部分，以使被攻击方认为自己收到的是合法的或被授权的报文。当某个节点复制另一个节点发到其他节点的报文，并在其后重发它们时，如果不能检测重发，目标节点会依据此报文的内容接受某些操作。例如，报文的内容是以前发过的口令，则将会出现严重的后果。

(4) 流量分析，指通过对网上信息流的观察和分析推断出网上的数据信息，例如有无传输，传输的数量、方向、频率等。因为网络信息系统的所有节点都能访问全网，所以流量的分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

(5) 破坏完整性，指有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改，使得接收方得到不正确的数据。

(6) 拒绝服务。当一个授权实体不能获得应有的对网络资源的访问或紧急操作被延迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议、超载或者某些特定的网络攻击引起。

(7) 资源的非授权使用,即与所定义的安全策略不一致的使用。因常规技术不能限制节点收发信息,也不能限制节点侦听数据,所以一个合法节点能访问网络上的所有数据和资源,为此,必须采用某些措施加以限制。

(8) 特洛伊木马,指非法程序隐藏在一个合法程序里从而达到其特定的目的(如盗取用户的敏感数据)。这可以通过替换系统合法程序,或者在合法程序里插入恶意代码来实现。

(9) 病毒。目前,全世界已经发现了上万种计算机病毒,而且新型病毒还在不断出现。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加,计算机病毒已经对计算机和网络构成了严重威胁。

(10) 诽谤,指利用网络信息系统的广泛互联性和匿名性,散布错误的消息以达到诋毁某人或某组织形象和知名度的目的。

1.2.3 信息安全问题的起源

信息安全问题是一个系统问题,而不是单一的信息本身的问题,因此要从信息系统的角度来分析组成系统的软硬件及处理过程中信息可能面临的风险。一般认为,系统风险是系统脆弱性或漏洞,以及以系统为目标的威胁的总称。系统脆弱性和漏洞是风险产生的原因,威胁或攻击是风险的结果。从另一个角度看,风险的客体是系统脆弱性和漏洞,风险的主体是针对客体的威胁或攻击。可见,当风险的因果或主客体在时空上一致时,风险就危及或破坏了系统安全,或者说信息系统处于不稳定、不安全状态中。

一个系统如果没有任何漏洞,任何攻击都不会产生影响;没有攻击,一个有漏洞甚至是较多漏洞的系统都可以安全运行。

计算机网络是目前信息处理的主要环境和信息传输的主要载体,特别是互联网的普及,给我们的信息处理方式带来了根本的变化。互联网的"无序、无界、匿名"三大基本特征也决定了网络信息的不安全性。综合起来说,信息安全的风险主要来自以下几个方面:物理因素、系统因素、网络因素、应用因素和管理因素。

1. 物理因素

计算机本身和外部设备乃至网络和通信线路面临各种风险,如各种自然灾害、人为破坏、操作失误、设备故障、电磁干扰、被盗和各种不同类型的不安全因素所致的物质财产损失、数据资料损失等。

2. 系统因素

1) 硬件组件

信息系统硬件组件的安全隐患多来源于设计,如生产工艺或制造商的原因,计算机硬件系统本身有故障(如电路短路、断线)、接触不良引起系统的不稳定、电压波动的干扰等。由于这种问题是固有的,一般除在管理上强化工作弥补措施外,采用软件方法见效不大。因此,在自制硬件或选购硬件时应尽可能避免或消除这类安全隐患。

2) 软件组件

软件的"后门"是软件公司的程序设计人员为了方便而在开发时预留设置的,它一方面为软件调试、进一步开发或远程维护提供了方便,但另一方面也为非法入侵提供了通道。这些"后门"一般不被外人所知,但一旦"后门"打开,其造成的后果将不堪设想。

此外，软件组件的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中的不必要的功能冗余以及软件过长、过大，不可避免地会存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，会导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，会导致产生垃圾软件，这种软件从安全角度看是绝对不可用的。

3. 网络因素

在当今的网络通信协议中，安全问题最多的是基于 TCP/IP 协议族的互联网及其通信协议。TCP/IP 协议族原本只考虑互通互联和资源共享的问题，并未考虑也无法兼容解决来自网络中和网际间的大量安全问题。TCP/IP 最初设计的应用环境是美国国防系统的内部网络，这一网络环境是互相信任的，在其推广到全社会的应用环境后，安全问题就发生了。概括来说，互联网网络体系存在如下几种致命的安全威胁。

1）缺乏对用户身份的鉴别

TCP/IP 协议的机制性安全隐患之一是缺乏对通信双方真实身份的鉴别机制。由于 TCP/IP 协议使用 IP 地址作为网络节点的唯一标识，而 IP 地址的使用和管理又存在很多问题，因而可导致下列两种主要安全隐患。

(1) IP 地址是由 InterNIC 分发的，其数据包的源地址很容易被发现，且 IP 地址隐含了所使用的子网掩码，攻击者据此可以画出目标网络的轮廓。因此，使用标准 IP 地址的网络拓扑对互联网来说是暴露的。

(2) IP 地址很容易被伪造和被更改，且 TCP/IP 协议没有对 IP 包中源地址真实性的鉴别机制和保密机制。因此，互联网上任一主机都可以产生一个带有任意源 IP 地址的 IP 包，从而假冒另一个主机进行地址欺骗。

2）缺乏对路由协议的鉴别认证

TCP/IP 协议在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护，因此可以通过互联网，利用路由信息修改网络传输路径，误导网络分组传输。

3）TCP/UDP 的缺陷

TCP/IP 协议规定了 TCP/UDP 是基于 IP 协议上的传输协议，TCP 分段和 UDP 数据包是封装在 IP 包中在网上传输的，除可能面临 IP 层所遇到的安全威胁外，还存在 TCP/UDP 实现中的安全隐患。

(1) 建立一个完整的 TCP 连接，需要经历“三次握手”过程，在客户机/服务器模式的“三次握手”过程中，假如客户机的 IP 地址是虚假的，是不可达的，那么 TCP 不能完成该次连接所需的“三次握手”，使 TCP 连接处于“半开”状态，攻击者利用这一弱点可实施如 TCP/SYN Flooding 攻击的“拒绝服务”攻击。

(2) TCP 提供可靠连接是通过初始序列号和鉴别机制来实现的。一个合法的 TCP 连接都有一个客户机/服务器双方共享的唯一序列号作为标识和鉴别。初始序列号一般由随机数发生器产生，但问题出在很多操作系统在实现 TCP 连接初始序列号的方法中，它所产生的序列号并不是真正随机的，而是一个具有一定规律、可猜测或计算的数字。对攻击者来说，猜出了初始序列号并掌握了目标 IP 地址后，就可以对目标实施 IP Spoofing 攻击，而 IP Spoofing 攻击很难检测，因此，此类攻击危害极大。

(3) 由于 UDP 是一个无连接控制协议，极易受 IP 源路由和拒绝服务型攻击。

4. 应用因素

主要是指使用者的习惯及方法不正确。据统计，10 种最危险的网络行为为：浏览不明邮件附件；安装未授权应用；关闭或禁用安全工具；浏览不明 HTML 或文本消息；浏览赌博、色情或其他非法站点；公开自己的密码、令牌或智能卡信息；重要的文档没有加密；随意访问未知、不可信站点；随意填写 Web 脚本、表格或注册页面；频繁访问聊天室或社交站点。

5. 管理因素

安全大师 Bruce Schneier 说："安全是一个过程，而不是一个产品。"也就是说，单纯依靠安全设备是不够的，它是一个汇集了硬件、软件、网络、人以及他们之间的相互关系和接口的系统。

网络与信息系统的实施主体是人，安全设备与安全策略最终要依靠人才能应用与贯彻。很多单位存在安全设备设置不合理、使用管理不当、没有专门的信息安全人员、系统密码管理混乱等现象，这时，防火墙、入侵检测、VPN 等设备就无法发挥应有的作用。因此，有人将信息安全策略称为"七分管理、三分技术"。

事实上，安全是一种意识，一个过程，而不是仅通过某种技术就能实现的。进入 21 世纪后，信息安全的理念发生了巨大的变化，目前倡导一种综合的安全解决方法：针对信息的生存周期，以"信息保障"模型作为信息安全的目标，即信息的保护技术、信息使用过程中的检测技术、信息受影响或攻击时的响应技术和信息受损后的恢复技术为系统模型的主要组成元素，简称 PDRR 模型，如图 1-1 所示。从技术角度看，PDRR 模型已经包含了信息安全的各个方面，在信息生命周期的各个环节都能对信息起到安全保障的作用。但在设计信息系统安全整体解决方案时，在 PDRR 保障模型的前提下，综合信息安全管理措施，实施立体化的信息安全防护，即整体解决方案＝PDRR 模型＋安全管理。

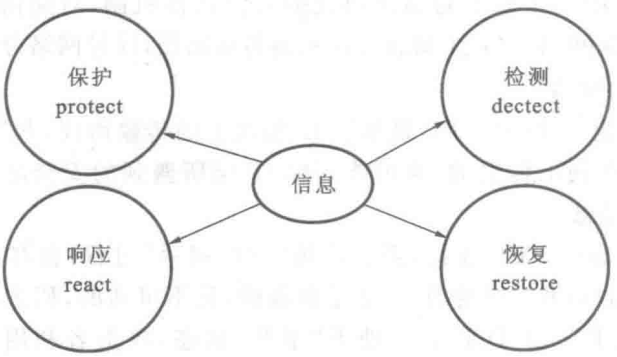

图 1-1　信息安全的 PDRR 模型

1.2.4　威胁和攻击的来源

1. 内部操作不当

当信息系统内部工作人员操作不当，特别是系统管理员和安全管理员出现管理配置的操作失误，就可能造成重大安全事故。