高等学校网络空间安全专业规划教材

“十二五”普通高等教育本科国家级规划教材

“十二五”江苏省高等学校重点教材

计算机网络安全

马利　姚永雷　编著

清华大学出版社

■ 高等学校网络空间安全专业规划教材

“十二五”普通高等教育本科国家级规划教材

“十二五”江苏省高等学校重点教材

计算机网络安全

马利　姚永雷　编著

清华大学出版社
北京

内 容 简 介

本书介绍网络安全基础理论及技术。全书共11章，详细讨论了密码学、消息鉴别和数字签名、身份认证、Internet安全、恶意代码及其防杀、防火墙、网络攻击与防范、虚拟专用网、无线网络安全和移动互联网安全。

本书内容反映了当前最新的网络安全理论与技术，既注重基础理论的介绍，又着眼于读者技术应用和实践能力的培养。

本书适合作为计算机专业本科生、大专生的计算机网络安全教材，也可供从事计算机网络安全工作的工程技术人员参考。

图书在版编目(CIP)数据

计算机网络安全/马利，姚永雷编著. —北京：清华大学出版社，2016
(高等学校网络空间安全专业规划教材)
ISBN 978-7-302-45667-4

Ⅰ. ①计… Ⅱ. ①马… ②姚… Ⅲ. ①计算机网络－网络安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第280065号

责任编辑：袁勤勇　战晓雷
封面设计：傅瑞学
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：19.5　　**字　数**：473千字
版　　次：2016年12月第1版　　**印　次**：2016年12月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：071489-01

前言

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。计算机网络的全球互联趋势越来越明显，其应用范围日渐普及和广泛，应用层次逐步深入。国家发展、社会运转以及人类的各项活动对计算机网络的依赖性越来越强。计算机网络已经成为人类社会生活不可缺少的组成部分。

与此同时，随着网络规模的不断扩大和网络应用的逐步普及，网络安全问题也越发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进和复杂化，已经严重威胁到网络和信息的安全。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

网络安全指网络系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，网络系统连续可靠正常地运行，网络服务不中断。从其本质上讲，网络安全就是网络上的信息安全。为了保证网络上信息的安全，首先需要自主计算机系统的安全；其次需要互联的安全，即连接自主计算机的通信设备、通信链路、网络软件和通信协议的安全；最后需要各种网络服务和应用的安全。从广义来说，凡是涉及网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全领域的相关理论和技术发展很快。为使读者全面、及时地了解和应用最新的网络安全技术，掌握网络安全的最新实践技能，编者在本书第 2 版的基础上进行了修订和补充。本次修订，保留和强化了实用性、体系结构、主线示例贯穿等特色，同时优化内容，淘汰陈旧知识、加入了当前最新的网络安全理论与算法；进一步扩充了网络安全实践的相关技术细节，并从知识内容优选、示例更新、实验体系扩展等多个方面进行修订，完善了理论教学内容，充实了实验指导。使得学生在系统学习基本概念、基本理论的基础上，深入理解并掌握常见网络安全防护技术。

本书以网络面临的常见安全问题以及相应的检测、防护和恢复为主线，系统地介绍了网络安全的基本概念、理论基础、安全技术及其应用。全书共

11章，内容包括计算机网络安全概述、密码学、消息鉴别和数字签名、身份认证、Internet安全、恶意代码及其防杀、防火墙、网络攻击与防范、虚拟专用网、无线网络安全、移动互联网安全等。希望通过本次修订，能够反映网络安全理论和技术的最新研究和教学进展，用通俗易懂的语言向读者全面而系统地介绍网络安全相关理论和技术，帮助读者建立完整的网络安全知识体系，掌握网络安全保护的实际技能。

本书内容完整，安排合理，难度适中；理论联系实际，原理和技术有机结合；逻辑性强，重点突出；文字简明，通俗易懂。本书可作为高等院校计算机及其相关专业的本科生、大专生的教材，也可作为网络管理人员、网络工程技术人员的参考书。

在本书的修订编写和申报“十二五”国家级规划教材的过程中得到了清华大学出版社的大力帮助和支持，在此表示由衷的感谢。

鉴于编者水平有限，书中难免出现错误和不当之处，殷切希望各位读者提出宝贵意见，并恳请各位专家、学者批评指正。作者的E-mail为ylyao@nusit.edu.cn。

本书配套课件可从清华大学出版社网站http://www.tup.tinghua.edu.cn下载。

编　者

2016年7月

目录

第 1 章 概　述

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越来越显著。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。计算机网络的全球互联趋势越来越明显，信息网络技术的应用日渐普及和广泛，应用层次逐步深入，应用范围不断扩展。基于网络的应用层出不穷，国家发展、社会运转以及人类的各项活动对计算机网络的依赖性越来越强。

但与此同时，网络安全问题越发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进和复杂化，令人防不胜防。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

1.1　网络安全挑战

计算机网络，尤其是 Internet，正面临着严重的安全挑战。Internet 是一个全球性的计算机互联网络，在发展初期规模不大，主要用于高等学校和科研院所，并假定用户之间存在信任关系，用户都是善意的。因此，Internet 在初期设计中几乎没有考虑安全方面的特性。但是，随着 Internet 规模逐渐扩大和用户数量的不断增长，这种信任模式已经逐步恶化。而且，以电子商务、电子政务为代表的新应用对网络安全提出了更高的要求。Internet 初期完全开放的设计特性而没有考虑安全的状况已经不能适应当代的需要。

1988 年莫里斯蠕虫病毒的发作使得 Internet 上超过 10%的计算机受害，之后每年重大网络安全事件不断发生。表 1-1 列出了历年的重大网络安全事件。

表 1-1　重大网络安全事件

事　件	时　间	影　响
梅丽莎(Melissa)	1999 年 5 月	一周内感染超过 100 000 台计算机，造成损失约 15 亿美元
爱虫(I Love You)病毒	2000 年 5 月	约 87 亿美元的经济影响
红色代码(Red Code)蠕虫	2001 年 7 月	14 小时内超过 359 000 台计算机被感染

续表

事　件	时　间	影　响
尼姆达(Nimda)蠕虫	2001 年 9 月	高峰时 160 000 台计算机被感染，超过 15 亿美元的经济影响
求职信(Klez)	2002 年	7.5 亿美元的经济影响
冲击波(Blaster)	2003 年	约 8 亿美元的经济影响
震荡波(Sasser)	2004 年 5 月	破坏能力和影响超过冲击波
极速波(Zobot)蠕虫	2005 年 8 月	具有像“冲击波”和“震荡波”一样的传播能力的恶意蠕虫，而且对反病毒厂商提出了公开挑战
熊猫烧香	2006 年	约 80 亿人民币的经济损失
灰鸽子	2005—2007 年	国内后门的集大成者，连续三次位列年度十大病毒
俄格网络战争	2008 年	俄罗斯与格鲁吉亚的冲突中，双方通过互联网相互攻击，开启了信息战争的先河
Conficker 蠕虫	2009 年	感染了超过数以千万计的计算机
“极光”漏洞	2010 年	导致谷歌网络被入侵，许多重要的知识财产被盗取
Facebook 被黑	2011 年	导致色情暴力图片泛滥
DNSChanger 肆虐	2012 年	全球 400 万台计算机被感染
Operation Last Resort 黑客行动	2013 年	Anonymous 黑客组织开展 Operation Last Resort 黑客行动，美国联邦政府无力招架
XX 神器	2014 年	一款手机木马，导致手机用户的手机联系人、身份证、姓名、各种账号等隐私信息泄露

近几年，安全攻击的复杂性提高了很多，攻击的自动化程度和攻击速度提高，杀伤力逐步增大；攻击工具的特征更难发现，更难利用特征进行检测。如红色代码和尼姆达这样的混合型威胁，使用组合的攻击方式快速进行传播，造成比单一型病毒更大的危害。2003 年 1 月的蠕虫王被释放后不到 10 分钟就感染了 75 000 台计算机。从世界范围看，网络入侵活动日益增加，并超过了恶意代码感染的次数。而且，入侵工具传播范围越来越广，入侵技术不断提高，对攻击者的知识要求反而降低了。当前，防火墙是人们用来防范入侵者的主要保护措施，但是越来越多的攻击技术可以绕过防火墙，不仅对广大用户，而且对 Internet 基础设施也将形成越来越大的威胁。

自 1994 年我国正式接入 Internet 以来，互联网在我国的规模和应用迅猛发展。2016 年 1 月中国互联网络信息中心(China Internet Network Information Center，CNNIC)发布的第 37 次中国互联网络发展状况统计报告显示，截至 2015 年 12 月底，中国网民规模达到 6.88 亿人，普及率达到 50.3%，年增长率为 2.4%。然而目前中国互联网安全情况不容乐观，各种网络安全事件层出不穷。综合来看，当前网络安全形势严峻的原因主要有以下三点：

(1) 由于近年来中国互联网持续快速发展，我国网民数量、宽带用户数量、.cn 域名数量都已经跃居全球第一位，而我国网络安全基础设施建设跟不上互联网发展的步伐，民众的网络安全意识薄弱，中小企业大多采用粗放式的安全管理风格，这三者相加直接导致中国互联网安全问题突出。

(2) 随着攻击技术的不断提高，攻击工具日益专业化、易用化，攻击方法也越来越复杂，越来越隐蔽，防护难度较大。

(3) 电子商务领域不断扩展，与现实中的金融体系日益融合，为网络世界的虚拟要素附加了实际价值，这些信息系统成为黑客攻击牟利的目标。

根据国家计算机病毒应急处理中心(CVERC)2016 年全国信息网络安全状况暨计算机和移动终端病毒疫情调查报告，2015 年我国计算机病毒感染率为 63.89%，64.22%的计算机用户发生过信息网络安全事件。在发生的网络安全事件中，病毒/木马高居首位，仍然是用户面临的最主要威胁；其次是垃圾邮件和网络钓鱼/网络欺诈。

攻击者攻击目标明确，针对网站和用户使用不同的攻击手段。对政府网站主要采用篡改网页的攻击形式，对企业则采用有组织的分布式拒绝服务(Distributed Denial of Service，DDoS)等攻击手段，对个人用户则通过窃取账号、密码等形式窃取用户个人财产，对金融机构则用网络钓鱼进行网络仿冒，在线盗取用户身份和密码。

当今社会，互联网已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用。随着我国政府信息化基础建设的推进和信息公开程度的提升，网络和信息安全也已成为关系到国家安全、社会稳定的重要因素，社会各界都对网络安全提出了更高的要求，采取有效措施，建设安全、可靠、便捷的网络应用环境，维护国家网络信息安全，成为社会信息化进程中亟待解决的问题。

1.2 网络安全的基本概念

1.2.1 网络安全的定义

计算机网络是利用通信线路把地理位置上分散的计算机和通信设备连接起来，在系统软件和协议的支持下，以实现数据通信和资源共享为目的的复杂计算机系统。网络的基本资源包括硬件资源、软件资源和数据资源等。

常见的安全术语有信息安全、网络安全、信息系统安全、网络信息安全、网络信息系统安全、计算机系统安全、计算机信息系统安全等。这些形形色色的说法，归根结底就是两层意思，即确保计算机网络环境下信息系统的安全运行，以及信息系统存储、处理和传输的信息受到安全保护。这些术语是殊途同归的关系。由于现代的信息系统大都建立在计算机网络基础上，计算机网络安全也就是信息系统安全。强调网络安全，主要由于计算机网络的广泛应用使得大部分信息都通过网络进行传输和处理，从而使得网络安全问题变得尤为突出。

网络安全指网络系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，网络系统连续可靠正常地运行，网络服务不

中断。

因此，网络安全同样也包括信息系统安全运行以及系统中的信息受到安全保护两个方面。从本质上讲，网络安全就是网络上的信息安全。为了保证网络上信息的安全，首先需要自主计算机系统的安全；其次需要互联的安全，即连接自主计算机的通信设备、通信链路、网络软件和通信协议的安全；最后需要各种网络服务和应用的安全。

网络安全的具体含义会随着利益相关方的变化而变化。

从一般用户（个人、企业等）的角度说，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能够保持机密性、完整性和真实性，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯自身的利益。

从网络运行者和管理者的角度说，他们希望对网络信息的访问受到保护和控制，避免出现非法使用、拒绝服务和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。

从安全保密部门的角度说，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，给国家造成巨大损失。

从社会教育和意识形态的角度说，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，必须对其进行控制。

1.2.2 网络安全的属性

根据网络安全的定义，网络安全具有以下几个方面的属性：

（1）机密性。保证信息与信息系统不被非授权的用户、实体或过程所获取与使用。

（2）完整性。信息在存储或传输时不被修改、破坏，或不发生信息包丢失、乱序等。

（3）可用性。信息与信息系统可被授权实体正常访问的特性，即授权实体在需要时能够存取所需信息。

（4）可控性。对信息的存储与传播具有完全的控制能力，可以控制信息的流向和行为方式。

（5）真实性。也就是可靠性，指信息的可用度，包括信息的完整性、准确性和发送人的身份真实性等方面，它也是信息安全性的基本要素。

其中，机密性、完整性和可用性通常被认为是网络安全的三个基本属性。

因此，从广义来说，凡是涉及网络上信息的机密性、完整性、可用性、可控性和真实性的相关技术和理论都是网络安全的研究领域。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。

1.2.3 网络安全层次结构

国际标准化组织（International Organization for Standards，ISO）提出了开放式系统互联（Open System Interconnection，OSI）参考模型，目的是成为计算机互连为网络的标准框架。但是，当前事实上的标准是 TCP/IP 参考模型。Internet 网络体系结构就以 TCP/IP 为核心。基于 TCP/IP 的参考模型将计算机网络体系结构分成 4 个层次，分别

是：网络接口层，对应 OSI 参考模型中的物理层和数据链路层；网际互连层，对应 OSI 参考模型的网络层，主要解决主机到主机的通信问题；传输层，对应 OSI 参考模型的传输层，为应用层实体提供端到端的通信功能；应用层，对应 OSI 参考模型的高层，为用户提供所需要的各种服务。

从网络安全角度，参考模型的各层都能够采取一定的安全手段和措施，提供不同的安全服务。但是，单独一个层次无法提供全部的网络安全特性，每个层次都必须提供自己的安全服务，共同维护网络系统中信息的安全。图 1-1 形象地描述了网络安全的层次。

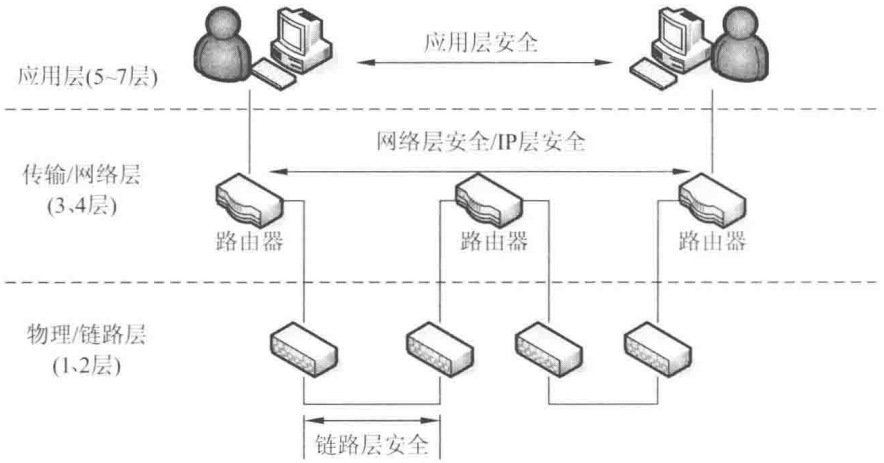

图 1-1 网络安全层次

在物理层，可以在通信线路上采取电磁屏蔽、电磁干扰等技术防止通信系统以电磁（电磁辐射、电磁泄漏）的方式向外界泄露信息。

在数据链路层，对点对点的链路可以采用通信保密机进行加密，信息在离开一台机器进入点对点的链路传输之前可以进行加密，在进入另外一台机器时解密。所有细节全部由底层硬件实现，高层无法察觉。但是这种方案无法适应经过多个路由设备的通信链路，因为在每台路由设备上都要进行加解密的操作，造成安全隐患。

在网络层，使用防火墙技术处理经过网络边界的信息，确定来自哪些地址的信息可以或者禁止访问哪些目的地址的主机，以保护内部网免受非法用户的访问。

在传输层，可以采用端到端的加密，即进程到进程的加密，以提高信息流动过程的安全性。

在应用层，主要是针对用户身份进行认证，并且可以建立安全的通信信道。

1.2.4 网络安全模型

图 1-2 给出了网络安全模型。消息从通信的一方（发送方）通过 Internet 传送至另一方（接收方），发送方和接收方是交互的主体，必须协调努力共同完成消息交换的任务。通过定义 Internet 上从发送方到接收方的路由以及双方共同使用的通信协议（如 TCP/IP）来建立逻辑信息通道。

当需要保护信息传输以保证信息的机密性、完整性、真实性的时候，就会涉及网络安

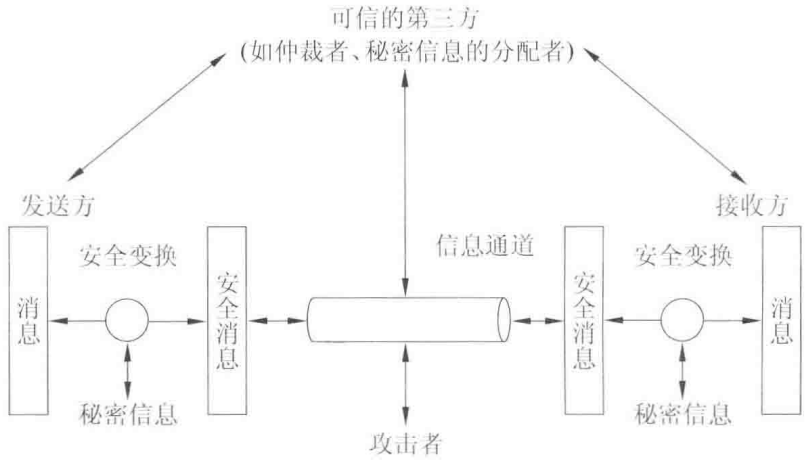

图 1-2 网络安全模型

全。一般来说,任何用来保证安全的方法都包含两个因素:

(1) 发送方对信息进行安全相关的转换。例如,对消息进行加密,即对消息进行变换,使得消息在传送过程中对攻击者不可读;或者将基于消息的编码附于消息后共同发送,以使接收方可以基于此编码验证发送方的身份。

(2) 双方共享某些秘密信息,并希望这些信息不为攻击者所知。如加密密钥,它配合加密算法在消息传输之前将消息加密,而在接收端将消息解密。

为了实现信息的安全传输,许多场合还需要有可信的第三方。例如,第三方负责将秘密信息分配给通信双方,而对攻击者保密;或者当通信双方关于信息传输的真实性发生争执时,由第三方来仲裁。

上述模型说明,设计网络安全系统时,应实现下列 4 个方面的任务:

(1) 设计一个算法用以实现和安全相关的变换。该算法应是攻击者无法攻破的。

(2) 产生算法所使用的秘密信息。

(3) 设计分发和共享秘密信息的方法,以保证该秘密信息不为攻击者所知。

(4) 设计通信双方使用的协议,该协议利用安全算法和秘密信息提供安全服务。

图 1-2 所示的网络安全模型虽是一个通用的模型,但是还有其他与安全有关的情形不完全符合该模型。例如,图 1-3 所示的网络访问安全模型可以保护信息系统拒绝非授权的访问。

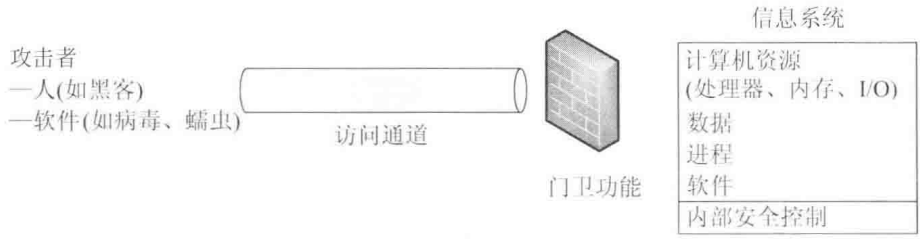

图 1-3 网络访问安全模型

应对非授权访问所需的安全机制分为两大类:第一类称为网闸功能,它包含基于口