普通高等教育“十一五”规划教材

网络信息安全技术概论（第二版）

吕林涛　主　编
张亚玲　吕　晖　李军怀　副主编

科学出版社
www.sciencep.com

普通高等教育“十一五”规划教材

网络信息安全技术概论

（第二版）

吕林涛　主　编

张亚玲　吕　晖　李军怀　副主编

科学出版社

北　京

内 容 简 介

本书系统介绍了计算机网络信息安全的基本理论和关键技术，主要内容包括：网络安全的基本概念、安全标准和网络安全防护体系、数据加密技术、密钥管理技术、数字签名和认证技术、黑客技术、漏洞扫描技术、入侵检测技术、Internet 的基础设施安全技术、防火墙技术、计算机病毒与恶意代码的防治、基于生物特征的身份认证技术、信息隐藏技术和网络信息审计技术等。本书的附录给出了近年来国家有关部门出台的网络安全方面的主要相关法规。

本书可作为高等学校信息安全、计算机科学与技术、信息管理和通信等专业及其他 IT 有关专业本科生和研究生的教材，也可作为从事网络信息安全技术的教学、科研和工程技术人员的参考书。

图书在版编目（CIP）数据

网络信息安全技术概论/吕林涛主编. —2 版. —北京：科学出版社，2010

（普通高等教育“十一五”规划教材）

ISBN 978-7-03-027380-2

Ⅰ.①网… Ⅱ.①吕… 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 077364 号

责任编辑：陈晓萍 / 责任校对：柏连海

责任印制：吕春珉 / 封面设计：东方人华

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

铭浩彩色印装有限公司 印刷

科学出版社发行 各地新华书店经销

*

2010 年 5 月第 一 版 开本：787×1092 1/16

2010 年 5 月第一次印刷 印张：21 1/2

印数：1—4 000 字数：506 000

定价：35.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

销售部电话 010-62134988 编辑部电话 010-62135120-8003

前　言

进入21世纪以来，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世纪发展的潮流和核心。Internet/Intranet 的发展，使得信息化带动了社会的工业化、现代化，网络技术为人类的进步作出了巨大的贡献。

网络的发展使人们可以通过一个终端与世界相连接，世界变得越来越小，人类的交往变得越来越便利，与此同时，个人机密数据、口令、银行账号等个人信息的隐私性安全问题日益凸显，这使得机遇与挑战并存。随着信息技术的发展，特别是计算机网络技术的发展，人们的诸多活动越来越多地依赖于网络空间，然而，网络空间并非总是安全的。

当前，我国的网络信息安全正面临着严峻的挑战。一方面随着电子政务工程的启动、电子商务的开展以及国家关键基础设施的网络化，网络安全的需要更加严格和迫切。另一方面，黑客攻击、病毒传播以及形形色色的网络攻击日益增加，网络安全防线十分脆弱。

因此，网络信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。网络安全不仅是一个技术问题，也是法律问题和社会问题，所以网络安全教育必须与信息教育同步开展。信息科技工作者除了要掌握专业技术以外，还应具有良好的网络文化道德，懂得网络管理的政策法规，能营造良好的网络文化氛围，不做网上违法的事情。所以，网络安全教育包括网络安全技术与网络安全法规两个方面。无疑网络信息安全问题的研究和技术的开发是现在和将来相当时期内重要的热点。

在计算机、信息学科的专业教育中开设网络信息安全的课程，旨在让学生们从一开始学习网络技术时就树立建立安全网络的观念，掌握网络安全的基本知识，了解设计和维护安全的网络体系及其应用系统的基本手段和常用方法，为从事信息网络的研究和开发打下良好的基础。

本书分为13章，通过对网络安全的基本概念、安全标准和网络安全防护体系、数据加密技术、密钥管理技术、数字签名和认证技术、黑客技术、漏洞扫描技术、入侵检测技术、Internet 的基础设施安全、防火墙技术、计算机病毒与恶意代码防治技术、基于生物特征的身份认证技术、信息隐藏技术和网络信息审计等技术的阐述，较全面地介绍了计算机网络信息安全的基本理论和关键技术；对当前常用的网络安全技术的原理和应用进行了详细的阐述，每章均附有习题。在此基础之上，基于生物特征的身份认证技术、信息隐藏技术和网络信息审计技术等可作为进一步学习的技术。为了加强网络法规的教育，在附录中提供了与网络安全相关的部分法规，供读者工作、学习参考之用。因此，本书既能够作为初学者的教材与自学用书，也可作为网络工作者常备的参考书。

本书的第2～4章由张亚铃撰写，第5、6、9、11章由吕林涛、吕晖撰写，第1、7章由李军怀撰写，第8章由张翔撰写，第10章由王永超撰写，第12章由赵明华撰写，第13章由张九龙撰写。全书由吕林涛教授和张亚玲副教授完成主要编写和统稿工作，

由王尚平教授审定。西安理工大学计算机学院研究生令小卓、石富旬、郝亮、洪磊、王金峰和杨玉林等参加了本书的相关工作。本书在编写过程中参考了许多相关的文献，在此一并表示感谢。

本书配有电子课件，课件由王金峰、杨玉林研究生完成，需要者可发邮件至cxp666@yeah.net 或 lvlintao@xaut.edu.cn 索取。

由于作者水平有限，编写时间仓促，对书中存在的错误和问题，殷切希望广大读者批评指正。

吕林涛

2010 年 4 月

目　录

第 1 章　网络安全概述

Internet/Intranet 技术的发展和普及，正在改变着世界经济、社会、文化的结构和运作方式，推动着各国的现代化，推动着社会文明的发展，改变着人们的思维方式。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互连性等特征，致使网络易受黑客、恶意软件和其他攻击，尤其不良网站严重侵蚀青少年的心灵健康等。使得计算机网络安全问题日益突出，网络安全已经涉及国民经济的各个领域，已经成为信息化建设的一个核心问题。

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。本章主要介绍网络安全的概念、威胁网络安全的因素、网络安全防护体系及网络安全的评估标准等方面的内容。

1.1　网络安全的基础知识

在社会日益信息化的今天，信息已经成为了一种重要的战略资源，信息的应用也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，在社会生产、生活中的作用日益显著。传播、共享和自增值是信息的固有属性，与此同时，又要求信息的传播是可控的、共享是授权的、增值是确认的。因此，信息的安全和可靠在任何状况下都是必须要保证的。信息网络的大规模全球互联趋势，Internet 的开放性，及人们的社会与经济活动对计算机网络依赖性的与日俱增，使得计算机网络的安全性成为信息化建设的一个核心问题。

以 Internet 为代表的全球性信息化浪潮日益高涨，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如政府部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在以下几个方面。

1）开放性的网络导致网络的技术是全开放的，任何一个人、团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如，可能是来自物理传输线路的攻击，也可以对网络通信协议和实现实施攻击；可以是对软件实施攻击，也可以对硬件实施攻击。

2）国际性的网络意味着网络的攻击不仅仅来自本地网络的用户，还可以来自 Internet 上的任何一台机器，也就是说，网络安全所面临的是一个国际化的挑战。

3）自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

尽管，开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得他们能够利用 Internet 提高办事效率和市场反应能力，以便

更具竞争力。通过 Internet，他们可以从异地取回重要数据，同时又要面对网络开放带来的数据安全的新挑战和新危险。如何保护政府、企事业的机密信息不受黑客和间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要事情之一。

1.1.1 网络安全的基本概念

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，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与原理，都是网络安全所要研究的领域。

网络安全是指网络系统的硬件、软件及其系统中的数据的安全，它体现于网络信息的存储、传输和使用过程。所谓的网络安全性就是网络系统的硬件、软件及其系统中的数据受到保护，不会由于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。

从不同的角度来说，网络安全具有不同的含义。从一般用户的角度来说，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、篡改等手段对用户信息的损害和侵犯，同时也希望用户信息不受非法用户的非授权访问和破坏。从网络运行和管理者角度来说，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，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，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，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

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，必须对其进行控制。

1.1.2 网络安全的特征

根据网络安全的定义，网络安全应具有以下六个方面的特征。

1）保密性：指信息不泄露给非授权的用户、实体及过程，或供其利用的特性。

2）完整性：指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

3）可用性：指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

4）可控性：指对信息的传播及内容具有控制能力，可以控制授权范围内的信息流向及行为方式。

5）可审查性：对出现的安全问题提供调查的依据和手段，用户不能抵赖曾做出的行为，也不能否认曾经接到对方的信息。

6）可保护性：保护软、硬件资源不被非法占有，免受病毒的侵害。

1.1.3 网络安全的目标

网络安全的目标是确保网络系统的信息安全。在网络系统中，任何调用指令和任何

信息反馈均是通过网络传输实现的，所以网络信息传输上的安全就显得特别重要。信息的传输安全主要是指信息在动态传输过程中的安全。为确保网络信息的传输安全，尤其需要防止如下问题。

（1）截获

对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获（Interception）与监听，进而得到用户或服务方的敏感信息。

（2）伪造

对用户身份伪造（Fabrication）这一常见的网络攻击方式，传统的对策一般采用身份认证方式来进行防护，但是，用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。身份认证的密码 90%以上是用代码形式传输的。

（3）篡改

攻击者有可能对网络上的信息进行截获并且篡改（Modification）其内容（增加、截去或改写），使用户无法获得准确、有用的信息或落入攻击者的陷阱。

（4）中断

攻击者通过各种方法，中断（Interruption）用户的正常通信，达到自己的目的。

（5）重发

信息重发（Repeat）的攻击方式，即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器（如银行的交易服务器）发送，以实现恶意的目的。

1.2　威胁网络安全的因素

计算机安全事业始于 20 世纪 60 年代。当时，计算机系统的脆弱性已日益为美国政府和私营的一些机构所认识。但是，由于当时计算机的速度和性能较落后，使用的范围也不广泛，再加上美国政府把它当作敏感问题而施加控制，因此，有关计算机安全的研究一直局限在比较小的范围内。进入 20 世纪 80 年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。并且，人们利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题。人们在这方面所作的研究与计算机性能和应用的飞速发展不相适应，因此，它已成为未来信息技术中的主要问题之一。

由于计算机信息有共享和易扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。

在计算机网络和系统安全问题中，常有的攻击手段和方式有：利用系统管理的漏洞直接进入系统；利用操作系统和应用系统的漏洞进行攻击；进行网络窃听，获取用户信息及更改网络数据；伪造用户身份、否认自己的签名；传输释放病毒和如 Java/ActiveX 控件来对系统进行有效控制；IP 欺骗；摧毁网络结点；消耗主机资源致使主机瘫痪和死机等。