全国应用型人才培养工程指定教材

IT技术类

网络信息安全与防护

IT技术类教材编写组　组编

杨佩璐　白　皓　主编

北京航空航天大学出版社

全国应用型人才培养工程指定教材
IT 技术类

网络信息安全与防护

IT 技术类教材编写组　组编
杨佩璐　白　皓　　主编

北京航空航天大学出版社

内 容 简 介

本书是作者根据全国应用型人才培养工程培养应用型人才的标准和要求，在长期从事“网络信息安全与防护”课程教学与应用开发的基础上编写的。全书共10章，主要内容包括计算机网络安全概述、网络协议基础、密码学基础、网络攻击与防护、防火墙技术、虚拟专用网、计算机病毒及防治知识、数据安全与备份技术、Web安全与电子商务知识和网络安全方案设计等。

本书既可作为高职高专院校各专业相关课程的教材，也可供网络应用和维护人员参考。

图书在版编目(CIP)数据

网络信息安全与防护/杨佩璐等主编. —北京：北京航空航天大学出版社，2009.9

ISBN 978-7-81124-871-5

Ⅰ.网… Ⅱ.杨… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2009)第138988号

网络信息安全与防护

IT技术类教材编写组 组编

杨佩璐 白 皓 主编

责任编辑 刘晓明

*

北京航空航天大学出版社出版发行

北京市海淀区学院路37号(100191) 发行部电话：010-82317024 传真：010-82328026

http://www.buaapress.com.cn E-mail:bhpress@263.net

北京时代华都印刷有限公司印装 各地书店经销

*

开本：787×1 092 1/16 印张：17 字数：435千字

2009年9月第1版 2009年9月第1次印刷 印数：5 000册

ISBN 978-7-81124-871-5 定价：30.00元

全国应用型人才培养工程
指定教材编委会

丛书前言

社会要发展，人才是关键。随着知识经济时代的到来，人才资源在经济发展中的地位和作用日益突出，已经成为现代经济社会发展的第一资源。目前，国内各行业对于应用型人才的需求日益迫切，无论是IT技术、工程制造领域，还是经济管理，甚至社会科学领域，都是如此。

全国应用型人才培养工程是由中外科教联合现代应用技术研究院组织开展的面向现代企业用人需要的人才工程。工程坚持“职业能力为导向，职业素质为核心”的课程设计原则，重点突出“职业精神、职业素质、职业能力”的培养，以提高学员的职业能力为目的，弥补技术人才与岗位要求的差距，提高学员的从业竞争力，培养适应现代信息社会需要的高技能应用型专业人才。

全国应用型人才培养工程包括培训、测评和就业三大部分。以企业对特定岗位的实际技术要求以及对从业人员的职业精神和素质要求为依据，通过课程嵌入或者集中培训的方式解决企业在岗前培训设置方面的诸多问题。人才工程还集合各专业、各方向社会普遍认可的考核、评测体系，通过整合及学分互认等方式，实现国家认证、国际学历的有益结合；实现职业资格、职业能力、专项技能和人才资格等多种认证的有益互补；实现紧缺人才库入库、技能大赛选拔以及人才择优推荐的有益支持，从而实现始于培训、专于认证、达于就业的完整的人才培养和服务体系。

全国应用型人才培养工程培训课程包括IT技术类、工程制造类、经济管理类和社会科学类4大类，13个专业方向，共100多门课程。

为了更好地配合全国应用型人才培养工程在全国的推广工作，我们专门成立了教材编写组，负责指定教材的编写工作。在编写过程中，依照人才工程所开设课程的考核标准，设定教材的编写纲目，分解知识点，选择常用经典实例，组织知识模块。

本套指定教材的特点体现在以下几个方面。

1. 行业特点

人才工程标准教材根据全国各级院校的专业教师、大中型培训机构培训师和企业相关技术人员提出的对新世纪本、专科学生培养的明确目标而设定内容，因此具备了明显的符合当前行业细分原则的侧重点与方向，更加符合企业用人的技术要求。

2. 内容侧重

人才工程主要解决当前本、专科学生所学知识内容与企业实际需要之间的差距问题；人才工程的指定教材则以企业对用人的实际技能需求为设定依据，按照“理论够用为度”的原则，对

各个专业的核心课程进行了梳理整合，并以实训内容为侧重点编写。因此，本套教材不仅适用于人才工程培训，亦适用于普通的本、专科院校。

3. 编写团队

全国应用型人才培养工程教研中心负责标准教材的组织和编写工作。本套教材由教研工作经验较为丰富的专业团队负责编写，既可以解决教学实践与工程案例的接口问题，也可以有效地提高实训教材的实用性。

4. 编写流程

注重整体策划。本套教材在策划以及编写过程中，严格按照“岗位群→核心技能→知识点→课程设置→各课程应掌握的技能→各教材的内容”的编写流程，保证了教学环节内容的设定和教材的编写与当前企业的实际工作需要紧密衔接。

为了方便教学，我们免费为选择本套教材的教师提供部分专业的整体教学方案以及教学相关资料：

◇ 所有教材的电子教案。

◇ 部分教材的习题答案。

◇ 部分教材的实例制作过程中用到的素材。

◇ 部分教材中实例的制作效果以及一些源程序代码。

本套教材的编写是在教育部、中国科学院、工业和信息化部、人力资源和社会保障部众多领导和专家的支持和帮助下才顺利完成的，在此我们表示衷心的感谢。同时，我们也欢迎读者朋友们能够对于本套教材给予指正和建议。来信请发至 napt. untis@gmail. com。

全国应用型人才培养工程指定教材编委会

2009 年 7 月

前　言

当今社会是一个信息社会，网络技术的迅猛发展使得信息的交流变得越来越便利。但是，在获得便利的同时，网络使用者也不得不面对网络中特别是 Internet 上日益突出的问题和威胁。这使得计算机网络安全及信息安全的问题成为人们关注的重点之一。

本书作为全国应用型人才培养工程指定教材之一，全面、系统地讲述了计算机网络信息的安全与防护知识。全书共分 10 章。第 1 章是计算机网络安全概述，使读者对于和网络安全相关的一些基础知识有一个基本的认识；第 2 章讨论网络协议的基础知识；第 3 章为密码学基础，着重介绍密码学领域中的多种技术及其应用，包括数据加密技术、数字签名技术及其应用等；第 4 章主要讲述网络攻击与防护的相关知识；第 5 章讲述防火墙技术的相关知识；第 6 章介绍虚拟专用网的相关内容；第 7 章讲述计算机病毒及防治知识；第 8 章是数据安全与备份技术，讲述其工作原理以及在网络中的应用等内容；第 9 章主要介绍 Web 安全与电子商务知识；第 10 章主要讲述网络安全方案设计的知识，让读者能够掌握网络安全方案设计方面的知识。

本书的编排组织充分体现了网络信息安全与防护的教学特点。每章节中对各知识点进行了深入的阐述，并且辅以相应的程序进行说明；每章的最后都配有针对性很强的习题。全书结构合理，详略得当，会对读者掌握网络信息安全与防护知识有很大的帮助。

本书的参考课时是 60 学时。

本书由杨佩璐、白皓主编。此外，参与本书编写的人员还有吴洪伟、徐振成、彭小琦、史磊、陈赞、李学俊等，在此表示衷心的感谢。

由于编写时间较为仓促，书中难免会有疏漏和不足之处，恳请广大读者提出宝贵意见。如果有任何的问题，可以通过电子邮件(wooystudio@263.net)与编者联系。

编　者

2009 年 7 月

目　录

第1章 计算机网络安全概述

本章要点

- 网络安全概述
- 网络安全的威胁
- 安全服务
- 安全机制
- 网络安全策略
- 网络安全体系

学习要求

- 了解计算机网络安全的概念和特征
- 了解计算机网络安全所面临的威胁
- 熟悉相关的安全服务和安全机制
- 熟悉计算机网络安全策略
- 掌握计算机网络体系知识

1.1 网络安全概述

当今，计算机网络所具有的信息共享和资源共享等优点，日益受到人们的关注并获得了广泛的应用。同时，Internet 应用范围的扩大，使得网络应用进入到一个崭新的阶段。一方面，入网用户能以最快的速度、最便利的方式以及最廉价的开销获得最新的信息，并在国际范围内进行交流；另一方面，随着网络规模越来越大和越来越开放，网络上的许多敏感信息和保密数据难免会遭受各种主动和被动的人为攻击。也就是说，人们在享受网络提供的好处的同时，也必须要考虑如何应对网络上日益泛滥的信息垃圾和非法入侵行为，即考虑网络安全问题。

1. 计算机网络安全的定义

计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因自然和人为的因素而受到破坏更改和泄露。网络安全主要包括物理安全、软件安全、信息安全和运行安全4个方面。

(1) 物理安全

物理安全包括硬件、存储媒体和外部环境的安全。

(2) 软件安全

软件安全指网络软件以及各个主机、服务器、工作站等设备所运行的软件的安全。

(3) 信息安全

信息安全指网络中所存储和传输数据的安全,主要体现在信息隐蔽性和防修改的能力上。

(4) 运行安全

运行安全指网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。

2. 计算机网络安全的特征

由于网络安全威胁的多样性、复杂性,以及网络信息、数据的重要性,在设计网络系统的安全时,应该努力达到安全目标。一个安全的网络具有下面5个特征:可靠性、可用性、保密性、完整性和不可抵赖性。

(1) 可靠性

可靠性是网络安全最基本的要求之一,是指系统在规定条件下和规定时间内完成规定功能的概率。

(2) 可用性

可用性是网络面向用户的基本安全要求。可用性是指信息和通信服务在需要时允许授权人或实体使用。网络最基本的功能是向用户提供所需的信息和通信服务,而用户的通信要求是随机的、多方面的,有时还要求时效性。

(3) 保密性

保密性指防止信息泄漏给非授权个人或实体,信息只为授权用户使用。保密性是面向信息的安全要求。

(4) 完整性

完整性也是面向信息的安全要求。它是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。

(5) 不可抵赖性

不可抵赖性也称做不可否认性,是面向通信双方(人、实体或进程)信息真实的安全要求。

1.2 网络安全的威胁

根据国际标准化组织定义的计算机网络面临的威胁,是对计算机网络安全性的潜在破坏。一个系统可能遭受到各种各样的威胁,只有知道系统遭受到的威胁以后,才能对其进行有效的防范。

计算机网络所面临的威胁可以分为两大类型,即主动威胁和被动威胁。

主动威胁是指威胁者对计算机网络信息进行修改、删除等非法操作;被动威胁是指威胁者通过非法手段获取信息、分析信息而不修改。

目前,计算机网络面临的安全性威胁主要有以下几个方面。

1. 非授权访问和破坏

非授权访问,即没有预先经过同意就使用网络或计算机资源。例如有意避开系统访问控制机制,对网络设备及资源进行非正常使用或者擅自扩大权限、越权访问信息等。这种威胁主要有以下几种表现形式:

① 假冒身份；

② 身份攻击；

③ 非法用户进入网络系统进行违法操作；

④ 合法用户以授权方式进行操作。

操作系统总不可避免地存在这样或那样的漏洞，一些别有用心的人就会利用系统中存在的漏洞进行网络攻击，其主要目标就是对系统数据的非法访问和破坏，例如人们熟知的“黑客”攻击。

2. 拒绝服务攻击

拒绝服务攻击(denial of service attack)是一种具有破坏性的攻击方式，最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时间内收到大量的电子邮件，使用户系统不能处理正常业务，严重时会使整个系统响应缓慢甚至瘫痪，影响正常用户的使用，甚至会导致合法用户被排斥而无法进入计算机网络系统或者无法使用相应的服务。

3. 计算机病毒

计算机病毒实际上是一段具有破坏性的程序，这种病毒程序具有极大的破坏性，其危害性已经为人们所认识。单机病毒已经让人们“谈毒色变”；而通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面，都是单机病毒所无法比拟的。

4. 特洛伊木马

特洛伊木马(Trojan horse)简称“木马”，据说这个名称来源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城，久久无法攻下。于是有人献计制造一只高两丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，大部队假装撤退而将木马摒弃于特洛伊城下。城中得知解围的消息后，遂将“木马”作为奇异的战利品拖入城内，全城饮酒狂欢。到午夜时分，全城军民进入梦乡，匿于木马中的将士开秘门游绳而下，开启城门及四处纵火，城外伏兵涌入，部队里应外合，焚屠特洛伊城。后世称这只大木马为“特洛伊木马”。如今黑客程序借用其名，有“一经潜入，后患无穷”之意。

完整的木马程序一般由两个部分组成：一个是服务器端，一个是控制器端。“中了木马”就是指安装了木马的客户端程序，若计算机中被安装了客户端程序，则拥有相应服务器端的人就可以通过网络控制该计算机为所欲为，这时计算机上的各种文件、程序，以及在计算机上使用的账号、密码就无安全可言了。

木马程序不能算是一种病毒，但可以和最新病毒、漏洞攻击工具一起使用，几乎可以躲过各大杀毒软件，尽管现在越来越多的新版杀毒软件可以查杀一些防杀木马了。所以不要认为使用有名的杀毒软件，计算机就绝对安全，木马永远是防不胜防的，除非不上网。

5. 破坏数据的完整性

它是指以非法手段窃得对数据的使用权，删除、修改、插入或者重发某些重要信息，可以修改网络上传输的数据，或者销毁网络上传输的数据，替代网络上传输的数据，重复播放某个分组序列，改变网络上传输的数据包的先后次序，使攻击者受益，却干扰了被侵害用户的正常使用。

6. 蠕 虫

它是指计算机病毒中的蠕虫(worms)病毒。

蠕虫病毒是一种常见的计算机病毒。它的传染机理是利用网络进行复制和传播，传染途径是网络、电子邮件以及U盘、移动硬盘等移动存储设备。比如2006年以来危害极大的“熊