21

高等学校信息工程类“十三五”规划教材

网络安全与保密

（第二版）

胡建伟　主编◎
马建峰　主审◎

WANGLUO ANQUAN YU BAOMI

西安电子科技大学出版社
http://www.xduph.com

高等学校信息工程类“十三五”规划教材

网络安全与保密

（第二版）

胡建伟　主编
马建峰　主审

西安电子科技大学出版社

内 容 简 介

网络安全和密码学是当今通信与计算机领域的热门课题。本书内容新颖而丰富，主要讲述了基本的密码学原理，各种加/解密算法及其应用，网络协议的安全漏洞和防护措施，系统安全技术，程序代码安全以及无线通信网络安全等内容。各章节都提供了大量的参考资料和习题，以供读者进一步学习、研究。

本书可作为高等院校信息对抗、通信、电子或计算机相关专业的教材，也可作为相关领域的研究人员和专业技术人员的参考书。

本书配套的幻灯片、实验材料以及引用的部分参考资料可以在网站 http: //see.xidian.edu.cn/hujianwei 下载。

★ 本书配有电子教案，有需要者可登录出版社网站，免费提供。

图书在版编目(CIP)数据

网络安全与保密/胡建伟主编. —2 版. —西安：西安电子科技大学出版社，2018.8

高等学校信息工程类“十三五”规划教材

ISBN 978-7-5606-3382-4

Ⅰ. ① 网… Ⅱ. ① 胡… Ⅲ. ① 计算机网络—安全技术—高等学校—教材 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2015）第 135855 号

策划编辑 马晓娟

责任编辑 马晓娟 董小兵

出版发行 西安电子科技大学出版社（西安市太白南路 2 号）

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com

经 销 新华书店

印刷单位 北京虎彩文化传播有限公司

版 次 2018 年 8 月第 2 版 2018 年 8 月第 5 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 20.25

字 数 479 千字

印 数 16 001～17 000 册

定 价 48.00 元

ISBN 978-7-5606-3382-4/TP

XDUP 3674002-5

序

第三次全国教育工作会议以来，我国高等教育得到空前规模的发展。经过高校布局和结构的调整，各个学校的新专业均有所增加，招生规模也迅速扩大。为了适应社会对“大专业、宽口径”人才的需求，各学校对专业进行了调整和合并，拓宽专业面，相应的教学计划、大纲也都有了较大的变化。特别是进入21世纪以来，信息产业发展迅速，技术更新加快。面对这样的发展形势，原有的计算机、信息工程两个专业的传统教材已很难适应高等教育的需要，作为教学改革的重要组成部分，教材的更新和建设迫在眉睫。为此，西安电子科技大学出版社聘请南京邮电学院、西安邮电学院、重庆邮电学院、吉林大学、杭州电子工业学院、桂林电子工业学院、北京信息工程学院、深圳大学、解放军电子工程学院等10余所国内电子信息类专业知名院校长期在教学科研第一线工作的专家教授，组成了高等学校计算机、信息工程类专业系列教材编审专家委员会，并且面向全国进行系列教材编写招标。该委员会依据教育部有关文件及规定对这两大类专业的教学计划和课程大纲，对目前本科教育的发展变化和相应系列教材应具有的特色和定位以及如何适应各类院校的教学需求等进行了反复研究、充分讨论，并对投标教材进行了认真评审，筛选并确定了高等学校计算机、信息工程类专业系列教材的作者及审稿人。

审定并组织出版这套教材的基本指导思想是力求精品、力求创新、好中选优、以质取胜。教材内容要反映21世纪信息科学技术的发展，体现专业课内容更新快的要求；编写上要具有一定的弹性和可调性，以适合多数学校使用；体系上要有所创新，突出工程技术型人才培养的特点，面向国民经济对工程技术人才的需求，强调培养学生较系统地掌握本学科专业必需的基础知识和基本理论，有较强的本专业的基本技能、方法和相关知识，培养学生具有从事实际工程的研发能力。在作者的遴选上，强调作者应在教学、科研第一线长期工作，有较高的学术水平和丰富的教材编写经验；教材在体系和篇幅上符合各学校的教学计划要求。

相信这套精心策划、精心编审、精心出版的系列教材会成为精品教材，得到各院校的认可，对于新世纪高等学校教学改革和教材建设起到积极的推动作用。

系列教材编委会

2002年8月

高等学校计算机、信息工程类专业规划教材编审专家委员会

前　言

2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，标志着我国正式将网络安全提升至国家安全的高度。网络空间逐渐成为继陆、海、空、天之后的“第五空间”，网络和信息安全已经成为国际社会关注的焦点和热点。网络空间在国际经济、政治中的地位日趋重要，网络安全形势更为复杂，加强网络安全已成为当务之急。

要想提升国家网络空间安全的整体实力，需要推动和普及信息安全全民教育水平。2015 年 6 月，“网络空间安全”正式获批成为国家一级学科，为信息安全人才的培养奠定了坚实的基础。本书的出版也是恰逢其时，旨在为我国网络安全人才的培养做出一份贡献。

本书作者长期从事网络安全教育培训工作，深知网络安全人才培养的不容易，也一直致力于建立和维护多层次、多种类、高水平的网络安全人才培养体系，通过多种形式发现和选拔网络安全人才。由于网络安全涉及计算机科学、网络技术、通信技术、密码技术、信息理论等多种学科，而且有很强的工程应用背景，要较好地掌握网络安全技术，需要读者有相当的自主学习能力和浓厚兴趣。本书也算是作者对自身长期安全教育工作的总结，希望能对有志于网络安全工作的读者起到抛砖引玉的作用。

全书从密码学、网络协议安全性、各类应用安全问题、系统安全机制、代码安全等方向重点阐述网络安全存在的安全隐患和对应的安全解决方案。全书尽可能从不同网络层次、不同用户角度阐释网络安全技术。

本次修订的主要内容包括：

(1) 增加了对网络安全体系结构和安全评估方法的介绍；

(2) 增加了对基本密码分析技术的讨论；

(3) 给出了指纹识别的基本原理；

(4) 增加了基于角色的访问控制技术；

(5) 增加了恶意代码的分析技术；

(6) 更多地用图形化方式表示安全的动态过程。

限于作者的水平，书中不当之处在所难免，诚恳期待广大读者提出宝贵意见。

胡建伟

2014 年 6 月

第一版前言

互联网与我们的生活息息相关，人们可以在网络允许的技术范围内，利用网络资源从事各种信息活动。在科学研究、技术开发、工农业、电子商务、教学、医疗保健、服务咨询、文化娱乐等几乎一切领域的信息处理和交换都可以利用网络来实现，从而大大地提高人类活动的质量和效率。但如同许多新技术的应用一样，网络技术也不啻是一柄人类为自己锻造的双刃剑，善意的应用将造福人类，恶意的应用则将给社会带来危害。

本书分六个部分来论述。

第一部分对网络安全所涵盖的基本概念进行了简单介绍，包括黑客群体、组网技术及其安全性、网络安全模型以及基本的安全技术等，使读者能尽快熟悉网络安全的相关知识。

第二部分分三章进行讨论，分别介绍了与密码学相关的理论知识，包括常规加密算法、公钥加密算法、散列函数和数字签名等。

第三部分按照互联网参考模型的协议层次结构由下往上分别进行讲述。其中，第5章根据 TCP/IP 协议存在的安全漏洞以及相应的攻击方法来讨论互联网的安全问题；第6～8章则依照 TCP/IP 存在的安全问题逐一讨论：第6章介绍了虚拟专用网和 IP 层安全协议，第7章叙述了传输层的安全套接层(SSL)协议，第8章论述了密码学理论的应用——身份认证和公钥基础设施(PKI)。

第四部分着重从系统的角度来讨论网络的安全性。其中，第9章以访问控制和系统审计为重点；第10章讲述了防火墙技术；第11章介绍了入侵检测系统，并分别从不同的角度对入侵检测技术进行了详尽的讨论。

第五部分主要研究软件（移动）代码的安全问题。其中，第12章重点介绍了缓存溢出、格式化字符串代码漏洞及预防办法；第13章介绍了移动代码安全技术；第14章介绍了恶意代码和计算机病毒。

第六部分对其它的安全主题进行了简单的介绍。其中，第15章讨论了流行的无线通信网的安全问题；第16章介绍了一种积极的网络安全防御技术：蜜罐主机和欺骗网络，其对间接提升网络的安全和预测新的网络入侵有着重要意义。

本书各章节都提供了大量参考资料以供读者进一步细查。本书配套的实验内容和幻灯片可以在网站 http://see.xidian.edu.cn/hujianwei 下载。

本书的参考教学时数为 40～50 学时，实验需另外安排。本书在选材上尽量做到少而精，而且尽量反映当前最新、最接近实际的网络安全技术。限于水平，书中难免有疏漏和错误之处，敬请广大读者批评指正。

参与本书编写的人员还有汤建龙(第二部分及第12、13章)和斯海飞(第9、11章)。

在编写本书的过程中，得到了西安电子科技大学电子对抗研究所众多同事的支持和帮助，在此深表谢意。

胡建伟

2003年8月

目　录

第1章 网络安全综述

1.1 安全的概念和术语

安全的最大问题是如何确定安全的度。拿一间私人住宅来说，我们可以设想出一系列安全性逐步递增的措施：

(1) 挂一窗帘以免让人从外面窥视到房子里的一举一动。

(2) 门上加锁，以免让小偷入内。

(3) 养一只大狼狗，将不受欢迎之人拒之门外。

(4) 警报系统，检测入侵的不速之客。

(5) 带电围墙、篱笆并增派门卫。

显然，我们可以有更多的安全措施。但是一般我们是基于以下三个因素来选择一个合适的安全目标：

(1) 安全威胁(如你的邻居是谁？)。

(2) 被保护物品的价值(如你有多少梵高的画？)。

(3) 安全措施所要达到的目标(objective)。

最后一个因素同另外两个相比较虽然不是很明显，但同等重要。同样是上面那个例子：如果我们的目标是保密性，那么最合适的安全措施应当是挂窗帘。

安全措施的目标主要有以下几类：

(1) 访问控制(Access Control)：确保会话对方(人或计算机)有权做他所声称的事情。

(2) 认证(Authentication)：确保会话对方的资源(人或计算机)同他声称的相一致。

(3) 完整性(Integrity)：确保接收到的信息同发送的一致。

(4) 审计(Accountability)：确保任何发生的交易在事后可以被证实。收发双方都认为交换发生过。即所谓的不可否认性(Non-repudiation)。

(5) 保密(Privacy)：确保敏感信息不被窃听，通常方法是加密。

所有这些目标同你所要传输的信息是密切相关的。

网络安全还必须考虑网络环境。网络环境包括在计算设备上运行的软件、在这些设备上存储以及传送的信息或这些设备生成的信息。容纳这些设备的设施和建筑也是网络环境的一部分。网络安全必须将这些因素考虑在内。

1.2 网络安全威胁

网络话题分散而复杂。网络的不安全因素，一方面是来自于其内在的特性——先天不

足。互联网连接着成千上万的区域网络和商业服务供应商的网络。网络规模增大，通信链路增长，网络的脆弱性(Vulnerability)和安全问题也随之增加。而且互联网在设计之初是以提供广泛的互连、互操作、信息资源共享为目的的，因此其侧重点并非在安全上。这在当初把互联网作为科学研究用途是可行的，但是在当今电子商务炙手可热之时，网络安全问题已经成为一种阻碍。另一方面是缺乏系统的安全标准。众所周知 IETF(Internet Engineering Task Force 因特网工程任务组)负责开发和发布互联网使用标准。随着互联网商业味道越来越浓，IETF 的地位变得越来越模糊不清。相反各个制造商为了各自的经济利益采用自己的标准，而不是遵循 IETF 的标准化进程。

1.2.1 脆弱性、威胁和风险

安全脆弱性是指系统设计、实现或运行中的、可被利用来破坏系统安全性的瑕疵或弱点(RFC 2828)。安全脆弱性不是风险、威胁或攻击。

弱点有四种类型。威胁型弱点来源于预测未来威胁(例如 7 号信令系统)的困难；设计和规范型弱点来源于协议设计中的错误或疏忽使其天生的不安全(例如 IEEE 802.11b 中的 WEP 协议)；实现型弱点是协议实现中的错误产生的弱点；运行和配置型弱点来源于实现时选项的错误使用或不恰当的布署政策(例如在网络中没有强制使用加密)。

根据 ITU-T X.800，安全威胁是对安全潜在的侵害，是危及信息系统环境安全的行为或事件。威胁有三个要素：

(1) 目标：可能受到攻击的一个安全方面。

(2) 作用者：进行威胁的人或机构。

(3) 事件：构成威胁的行为类型，是威胁的作用者可能对机构造成损害的方式。

威胁既可能是主动性的(当系统状态可被改变时)，又可能是被动性的(不改变系统状态但非法泄露信息)。伪装成合法主体和拒绝服务是主动性威胁的例子，窃听获取口令是被动性威胁的例子。威胁方可能是黑客、恐怖分子、破坏分子、有组织犯罪或政府发起的，但相当数量的威胁来自组织内部人员。

安全风险来源于安全脆弱性与安全威胁的结合。例如，操作系统应用的溢出漏洞(即脆弱性)加上黑客的知识、合适的工具和访问(即威胁)可产生万维网服务器攻击的风险。安全风险的后果是数据丢失、数据损坏、隐私失窃、诈骗、宕机及失去公共信任。

1.2.2 网络威胁的类型

威胁定义为对脆弱性的潜在利用，这些脆弱性可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏。网络安全与保密所面临的威胁可以来自很多方面，并且是随着时间的变化而变化。网络安全的威胁可以是来自内部网或者外部网，根据不同的研究结果表明，大约有 80%～95%的安全事故来自内部网。显然只有少数网络攻击是来自互联网。一般而言，主要的威胁种类有：

(1) 窃听或者嗅探：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。对广播网络的基带同轴电缆或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