网络空间安全专业规划教材

总主编◎杨义先　　执行主编◎李小勇

无线通信安全

Security of Wireless Communication

主编 李 晖

北京邮电大学出版社
www.buptpress.com

划教材

总主编　杨义先　　执行主编　李小勇

无线通信安全

主编　李　晖


北京邮电大学出版社
www.buptpress.com

内容简介

本教材全面深入地介绍了无线通信安全的相关基础理论，重点讨论了第二代到第四代移动通信系统及无线局域网中的各项关键安全技术。全书共分为3个部分：第1部分是入门篇，介绍了无线通信及无线通信安全的历史和基本概念；第2部分是理论篇，介绍了无线通信安全的理论基础，包括密码学概述、序列密码、分组密码、公钥密码、数字签名、认证理论基础和密钥管理等；第3部分是实例篇，介绍了各种无线通信网络（如GSM、GPRS、窄带CDMA、WCDMA、LTE、TETRA、WLAN、WiMax和蓝牙等）的安全技术，包括认证、加密和密钥管理等。每章最后给出了习题，便于读者巩固、总结和运用书中的知识。

本教材适合作为高校网络空间安全相关专业的本科及研究生教材，也可以作为对无线通信安全、密码学应用、信息安全等内容感兴趣的技术人员或科研人员的参考读物。

图书在版编目(CIP)数据

无线通信安全 / 李晖主编. -- 北京 : 北京邮电大学出版社, 2018.10
ISBN 978-7-5635-5500-0

Ⅰ. ①无… Ⅱ. ①李… Ⅲ. ①无线电通信－安全技术 Ⅳ. ①TN92

中国版本图书馆CIP数据核字（2018）第159119号

书　　名：无线通信安全
作　　者：李　晖
责任编辑：刘　颖
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京博图彩色印刷有限公司印刷
开　　本：787 mm×1 092 mm　1/16
印　　张：21.75
字　　数：560千字
版　　次：2018年10月第1版　2018年10月第1次印刷

ISBN 978-7-5635-5500-0　　定　价：52.00元

Prologue 序

Prologue

作为最新的国家一级学科，由于其罕见的特殊性，网络空间安全真可谓是典型的“在游泳中学游泳”。一方面，蜂拥而至的现实人才需求和紧迫的技术挑战，促使我们必须以超常规手段，来启动并建设好该一级学科；另一方面，由于缺乏国内外可资借鉴的经验，也没有足够的时间纠结于众多细节，所以，作为当初“教育部网络空间安全一级学科研究论证工作组”的八位专家之一，我有义务借此机会，向大家介绍一下 2014 年规划该学科的相关情况，并结合现状，坦诚一些不足，以及改进和完善计划，以使大家有一个宏观了解。

我们所指的网络空间，也就是媒体常说的赛博空间，意指通过全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间。它已成为继陆、海、空、太空之后的第五空间。网络空间里不仅包括通过网络互联而成的各种计算系统（各种智能终端）、连接端系统的网络、连接网络的互联网和受控系统，也包括其中的硬件、软件乃至产生、处理、传输、存储的各种数据或信息。与其他四个空间不同，网络空间没有明确的、固定的边界，也没有集中的控制权威。

网络空间安全，研究网络空间中的安全威胁和防护问题，即在有敌手对抗的环境下，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施，以及网络和系统本身的威胁和防护机制。网络空间安全不仅包括传统信息安全所涉及的信息保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。

网络空间安全一级学科，下设五个研究方向：网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全。

方向 1，网络空间安全基础，为其他方向的研究提供理论、架构和方法学指导；它主要研究网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等内容。

方向2，密码学及应用，为后三个方向（系统安全、网络安全和应用安全）提供密码机制；它主要研究对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等内容。

方向3，系统安全，保证网络空间中单元计算系统的安全；它主要研究芯片安全、系统软件安全、可信计算、虚拟化计算平台安全、恶意代码分析与防护、系统硬件和物理环境安全等内容。

方向4，网络安全，保证连接计算机的中间网络自身的安全以及在网络上所传输的信息的安全；它主要研究通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等内容。

方向5，应用安全，保证网络空间中大型应用系统的安全，也是安全机制在互联网应用或服务领域中的综合应用；它主要研究关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等内容。

从基础知识体系角度看，网络空间安全一级学科主要由五个模块组成：网络空间安全基础、密码学基础、系统安全技术、网络安全技术和应用安全技术。

模块1，网络空间安全基础知识模块，包括：数论、信息论、计算复杂性、操作系统、数据库、计算机组成、计算机网络、程序设计语言、网络空间安全导论、网络空间安全法律法规、网络空间安全管理基础。

模块2，密码学基础理论知识模块，包括：对称密码、公钥密码、量子密码、密码分析技术、安全协议。

模块3，系统安全理论与技术知识模块，包括：芯片安全、物理安全、可靠性技术、访问控制技术、操作系统安全、数据库安全、代码安全与软件漏洞挖掘、恶意代码分析与防御。

模块4，网络安全理论与技术知识模块，包括：通信网络安全、无线通信安全、IPv6安全、防火墙技术、入侵检测与防御、VPN、网络安全协议、网络漏洞检测与防护、网络攻击与防护。

模块5，应用安全理论与技术知识模块，包括：Web安全、数据存储与恢复、垃圾信息识别与过滤、舆情分析及预警、计算机数字取证、信息隐藏、电子政务安全、电子商务安全、云计算安全、物联网安全、大数据安全、隐私保护技术、数字版权保护技术。

其实，从纯学术角度看，网络空间安全一级学科的支撑专业，至少应该平等地包含信息安全专业、信息对抗专业、保密管理专业、网络空间安全专业、网络安全与执法专业等本科专业。但是，由于管理渠道等诸多原因，我们当初只重点考虑了信息安全专业，所以，就留下了一些遗憾，甚至空白，比如，信息安全心理学、安全控制论、安全系统论等。不过值得庆幸的是，学界现在已经开始着手，填补这些空白。

北京邮电大学在网络空间安全相关学科和专业等方面，在全国高校中一直处于领先水平，从20世纪80年代初至今，已有30余年的全方位积累，而且，一直就特别重视教学规范、课程建设、教材出版、实验培训等基本功。本套系列教材主要是由北京邮电大学的骨干教师们，结合自身特长和教学科研方面的成果，撰写而成。本系列教材暂由《信息安全数学基础》《网络安全》《汇编语言与逆向工程》《软件安全》《网络空间安全导论》《可信计算理论与技术》《网络空间安全治理》《大数据服务与安全隐私技术》《数字内容安全》《量子计算与后量子密码》《无线通信安全》《移动终端安全》《漏洞分析技术实验教程》《网络安全实验》《网络空间安全基础》《信息安全管理（第3版）》《网络安全法学》《信息隐藏与数字水印》等20余本本科生教材组成。这些教材主要涵盖信息安全专业和网络空间安全专业，今后，一旦时机成熟，我们将组织国内外更多的专家，针对信息对抗专业、保密管理专业、网络安全与执法专业等，出版更多、更好的教材，为网络空间安全一级学科提供更有力的支撑。

杨义先

教授、长江学者

国家杰出青年科学基金获得者

北京邮电大学信息安全中心主任

灾备技术国家工程实验室主任

公共大数据国家重点实验室主任

2017年4月，于花溪

前言

Foreword

自20世纪70年代末第一代通信系统问世以来，移动通信技术发展迅速，特别是与有线因特网连接起来后，移动通信网络为用户提供“永远在线”、高速率的网络服务，用户不仅可以使用移动终端随时、随地与人交流，还可以使用移动终端浏览新闻、查询信息、网上购物、导航及进行移动支付等。

与此同时，移动通信系统普遍采用的无线通信技术本身固有的开放性使得它更容易受到监听、滥用等安全威胁，导致手机用户的通信记录（语音、短信、通话人、通话时间等信息）以及存储的机密信息（如银行账号、密码等重要资料）等的泄露，虚假基站也使得用户容易收到垃圾短信等。这些由于使用无线设备或技术带来的安全问题使用户的隐私和通信安全受到了极大的威胁，不仅破坏了社会的和谐与稳定，而且还威胁到了国家安全。因此，研究无线通信安全技术的理论、设计和完善无线通信网络安全是无线通信技术飞速发展的前提，是保障通信安全的关键，是国家信息安全建设的重点。

本教材深入地介绍了无线通信安全的相关基础理论与各项关键技术，主要围绕无线通信网络安全展开讨论。我们将从认识无线通信技术开始，逐步介绍无线通信网络所面临的安全威胁、要达到的安全要求和采取的安全措施。正如密码学理论是信息安全的基础一样，大部分的无线通信网络的安全措施依赖于密码学的基本理论，如加解密理论和认证理论。因此，本教材将密码学的基本理论作为无线通信安全的理论基础，进行较为详细的介绍，并在此基础上介绍目前主要的无线通信网络（包括第二代移动通信系统、第三代移动通信系统、LTE系统、无线集群通信系统、无线局域网、无线城域网等）采用的安全技术。

本教材共分为3个部分：第1部分是入门篇，由第1章和第2章组成，分别介绍无线通信和无线通信安全的历史、分类和基本概念；第2部分是理论篇，由第3～11章组成，主要介绍无线通信安全的理论基础——密码学的基础知识，包括密码学概述、序列密码、分组密码、公钥密码、数字签名、认证理论基础和密钥管理等；第3部分是实例篇，由第12～21章组成，包括GSM、GPRS、窄带CDMA、WCDMA、LTE、TETRA、WLAN、WiMax和蓝牙等的安全技术，主要介绍这些实际通信系统如何进行认证及管理密钥，如何保证传输的信息不被非法破译和篡改等。

本教材较完整地描述了无线通信系统中的信息安全基本理论与技术，读者既可以按顺序阅读本教材，也可以先跳过理论篇，直接阅读实例篇，而在理解某类无线通信系统安全技术遇到困难时再翻看前面的理论知识。本教材可以作为本科高年级学生和研究生的专业教材，参考学时为68学时。此外，本教材也可以供从事相关领域研究的科研人员阅读参考。相信本教材的深度和广度，可以方便不同层次的读者从书中的理论及技术论述中找到感兴趣的知识或答案。

本教材的策划以及主要章节的撰写、统稿和修改工作由李晖负责，特别要说明的是，本教材的完成是在作者2010年编写的《无线通信安全理论与技术》一书的基础上进行的，相关章节的内容保留了该书的部分内容，因此对参加编写该书的相关人员的辛勤工作表示感谢！另外，潘雪松、陈泽、马倩华、王鑫泺、范立岩、陈泽伦、冯皓楠和韩明哲参与了全书的校对工作，北京邮电大学出版社的马晓仟为本教材的出版付出了辛勤而有效的劳动，在此一并表示感谢。

本教材在编写过程中还参阅了国内外同行的大量文献，在此向这些文献的作者表示由衷的感谢！

鉴于无线通信及信息安全的理论与技术处在不断发展和完善之中，加之作者水平所限，本教材难免出现疏漏，甚至错误，恳请各位专家、学者和热心读者指正，并提出宝贵意见。我的电子邮箱是lihuill@bupt.edu.cn。

李　晖

2018年6月于北京邮电大学

目录

Contents

Contents

第 1 部分　入门篇

第 2 部分 理论篇

第 3 部分 实例篇