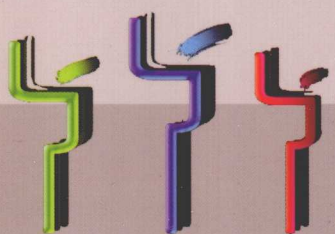
AnQuan

普通高校信息安全系列教材

李 晖 牛少彰 编 著

无线通信安全理论与技术

WUXIAN TONGXIN ANQUAN LILUN YU JISHU



北京邮电大学出版社
www.buptpress.com

普通高校信息安全系列教材

无线通信安全理论与技术

李　晖　牛少彰　编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书主要围绕无线通信安全的主要理论与技术进行研究和讨论。本书共分 4 部分，第 1 部分是入门篇，包括第 1，2 章，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 3～8 章组成，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、对称密码体制、公钥密码体制（非对称密码体制）、认证理论基础、数字签名、安全协议等内容；第 3 部分是实例篇，由第 9～17 章组成，内容包括 GSM，GPRS，窄带 CDMA，WCDMA，TETRA 等移动通信网络的安全技术，以及 WLAN，Ad Hoc，WiMAX 和蓝牙等无线通信网络的安全技术；第 4 部分是进展篇，由第 18～21 章组成，介绍移动可信计算、移动电子商务安全、传感器网络安全和移动数字版权保护等相关内容。

本书适合作为高校信息安全相关专业的本科及研究生教材，也可作为对密码学、信息安全、通信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

无线通信安全理论与技术/李晖，牛少彰编著. --北京：北京邮电大学出版社，2011.9
ISBN 978-7-5635-2688-8

Ⅰ.①无… Ⅱ.①李…②牛… 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（2011）第 146047 号

书　　名：无线通信安全理论与技术
作　　者：李　晖　牛少彰
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：北京联兴华印刷厂
开　　本：787 mm×960 mm　1/16
印　　张：23.25
字　　数：496 千字
印　　数：1—3 000 册
版　　次：2011 年 9 月第 1 版　2011 年 9 月第 1 次印刷

ISBN 978-7-5635-2688-8　　定价：42.00 元

前　言

随着移动通信技术的发展，通信网络正一步步向下一代移动互联网发展，即蜂窝移动网络、自组网(Ad Hoc)、无线局域网(WLAN)等多种无线网络实现动态的网络接入，再与有线互联网连接起来为用户提供“永远在线”、高速率的网络服务，使得用户不仅可以做到随时、随地与任何人交流，还可以随时、随地地访问互联网或企业内部网，完成信息浏览、网络银行、电子商务等功能。

无线通信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。例如，由Google自曝在香港用摄影车拍摄街景时，搜集并保存了部分市民通过无线网络(Wi-Fi)传送的未加密数据，比如电子邮件内容；2010年出现的手机卧底软件，可以将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)发到指定的监视网站上；从2004年全球出现首个手机病毒以来，手机病毒层出不穷，其危害涉及恶意扣费、窃取隐私、狂发短信等。这些由于使用无线设备或技术而出现的新的安全事件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的安全机制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。

本书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，比如，加解密理论和认证理论，因此，本书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，在此基础上介绍目前主要的无线通信网络采用的安全技术，包括第二代移动通信系统、第三代移动通信系统、无线集群通信系统、无线局域网、无线城域网等，最后将介绍无线通信安全的最新技术。

全书共分4部分，第1部分是入门篇，包括第1章和第2章，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3～8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、对称密码体制、公钥密码体制(非对称密码体制)、认证理论基础、数字签名、安全协议等内容；第3部分是实例篇，由第9～17章组成，内容包括GSM，GPRS，窄带CDMA，WCDMA，TETRA等移动通信网络的安全技术，以及WLAN，Ad Hoc，WiMAX和蓝牙等无线通信网络的安全技术；

第4部分是进展篇，介绍无线通信技术的最新进展，由第18～21章组成，分别介绍移动可信计算、移动电子商务安全、传感器网络安全和移动数字版权保护等相关内容。

本书可以作为本科高年级学生和研究生的专业教材，参考学时数为68学时。此外，本书也可以供从事相关领域研究的科研人员阅读参考。

本教材的策划、主要章节的撰写、统稿和修改工作由李晖负责。参加编写的主要人员有牛少彰、李冰、刘志国、闫海成、施腾飞、程琳静、陈乐等，另外胡也、陈佳康、王榕、夏伟、张莹、白云和邓冠阳参与了本书的校对工作，在此对他们的辛勤工作表示感谢！

本书在编写过程中还参阅了国内外同行的大量文献，在此向文献的作者表示由衷的感谢！

由于作者水平有限，书中难免出现疏漏，甚至错误，恳请广大同行和读者指正，并提出宝贵意见，以便我们再版时修改和完善。我的电子邮箱是 lihuill@bupt.edu.cn。

李　晖

2011年7月于北京邮电大学

目　录

第 1 部分　入门篇

第 2 部分 理论篇

第3部分 实例篇

第 4 部分 进展篇

第1部分　入门篇

飞速发展的移动通信技术、功能多样的卫星服务、不断完善的无线局域网技术正对通信和网络产生巨大的改变，使人们的生活越来越多地依赖于手机、PDA等无线移动终端。这些通信技术的核心就是无线技术，它已经成为电信业和网络界最激动人心的领域。无线代表着无拘无束，人们可以不受时间、地点的限制与其他人沟通或者进行信息交换，这种无拘无束同时也给信息安全带来了难题。本书将带领大家认识无线通信网络，了解无线通信网络中存在的安全问题，探讨保护无线通信安全的基本理论和主要技术。

作为本书的第1部分，先来认识一下什么是无线通信，它面临着哪些安全问题，提出了哪些安全要求。