

AnQuan

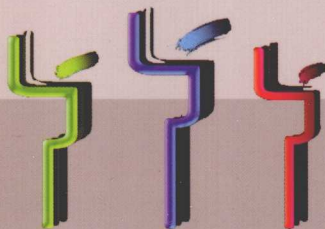
普通高校信息安全系列教材



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

TN92/150

2011

无线通信安全理论与技术

李 晖 牛少彰 编著

北方工业大学图书馆



C00272413



北京邮电大学出版社
[www. buptpress. com](http://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—3000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

· 如有印装质量问题,请与北京邮电大学出版社营销中心联系 ·

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 1 章 无线通信入门	3
1.1 无线通信的历史	3
1.2 无线通信基本技术	5
1.2.1 射频基础	5
1.2.2 无线传输介质	6
1.2.3 传统无线技术	7
1.3 无线通信网络分类	10
1.4 无线通信的研究机构和组织	12
1.4.1 中国通信标准化协会	12
1.4.2 国际电信联盟	14
1.4.3 美国联邦通信委员会	15
1.4.4 欧洲邮电通信管理协会	16
1.4.5 电气和电子工程师协会	16
1.4.6 Wi-Fi 联盟	18
第 2 章 无线通信安全入门	19
2.1 无线通信安全历史	19
2.2 无线通信网的主要安全威胁	22
2.2.1 对传递信息的威胁	23
2.2.2 对用户的威胁	25
2.2.3 对通信系统的威胁	25
2.3 移动通信系统的安全要求	26
2.4 移动通信系统的安全体系	27



2.4.1 安全服务	28
2.4.2 安全需求	30
2.4.3 安全域	31

第2部分 理论篇

第3章 密码学概述	35
3.1 密码学的基本概念	35
3.2 密码体制分类	37
3.3 古典密码简介	38
3.3.1 单码加密法	39
3.3.2 多码加密法	40
3.3.3 经典多图加密法	41
3.3.4 经典换位加密法	42
3.4 密码体制安全性	42
第4章 对称密码体制	45
4.1 序列密码概述	45
4.1.1 序列密码的基本概念	46
4.1.2 序列密码的分类	48
4.1.3 密钥流生成器的结构	50
4.2 典型序列密码算法	52
4.2.1 A5 算法	52
4.2.2 RC4 算法	53
4.3 分组密码理论	56
4.3.1 分组密码概述	57
4.3.2 分组密码算法的设计原则	58
4.3.3 SPN 结构简介	59
4.3.4 密钥扩展算法的设计原则	60
4.4 典型分组密码算法	61
4.4.1 DES 算法	61
4.4.2 AES 算法	70
4.4.3 国际数据加密算法(IDEA)	78



4.5 密码运行模式	82
4.5.1 电子密码本(ECB)模式	82
4.5.2 密码分组链接(CBC)模式	84
4.5.3 密码反馈(CFB)模式	86
4.5.4 输出反馈(OFB)模式	87
4.5.5 计数器(CTR)模式	89
4.5.6 选择密码模式	90
第5章 公钥密码体制	93
5.1 公钥密码的基本概念	93
5.1.1 问题的复杂性理论	93
5.1.2 公钥密码的原理	95
5.1.3 公钥密码的使用	96
5.2 RSA 密码体制	96
5.2.1 RSA 算法描述	97
5.2.2 RSA 算法举例	97
5.2.3 RSA 算法实现	98
5.2.4 RSA 算法的常见攻击	98
5.3 椭圆曲线密码体制	99
5.3.1 椭圆曲线概念	99
5.3.2 椭圆曲线密码算法	102
5.3.3 椭圆曲线密码算法实例	103
5.3.4 椭圆曲线密码算法的安全性	104
5.4 NTRU 公钥密码	104
5.4.1 NTRU 基于的困难问题	105
5.4.2 NTRU 算法描述	106
5.4.3 NTRU 算法举例	107
第6章 认证理论基础	109
6.1 认证的基本概念和认证系统的模型	109
6.2 认证函数	110
6.2.1 信息加密函数	111
6.2.2 信息认证码	112
6.3 杂凑函数	115



6.3.1	杂凑函数的定义	116
6.3.2	杂凑函数的基本用法	116
6.3.3	杂凑函数通用模型	118
6.3.4	构造杂凑函数	118
6.3.5	对杂凑函数的攻击	119
6.4	MD4 和 MD5 算法	120
6.4.1	算法简介	120
6.4.2	MD5 算法描述	121
6.4.3	MD5 算法安全性	123
6.5	安全杂凑算法(SHA)	123
6.5.1	SHA 算法描述	123
6.5.2	SHA 算法安全性	125
第 7 章	数字签名	127
7.1	数字签名基本概念	127
7.2	常用数字签名技术简介	129
7.2.1	RSA 数字签名方案	129
7.2.2	DSS 数字签名标准	130
7.3	特殊数字签名	132
7.3.1	一次性数字签名	132
7.3.2	群签名	132
7.3.3	代理签名	133
7.3.4	盲签名	134
7.3.5	多重签名	135
第 8 章	安全协议	137
8.1	安全协议概述	137
8.1.1	安全协议的概念	137
8.1.2	安全协议的安全性	139
8.1.3	安全协议设计规范	140
8.1.4	协议的形式化证明	141
8.1.5	安全协议的常见攻击和相应对策	143
8.2	身份认证协议	145
8.2.1	身份认证的概念	145



8.2.2 零知识身份认证协议	146
8.2.3 询问应答协议	147
8.2.4 认证协议向数字签名方案的转换	148
8.3 密钥建立协议	149
8.3.1 密钥协商协议	149
8.3.2 密钥分配协议	151
8.3.3 密钥更新协议	153

第 3 部分 实例篇

第 9 章 GSM 系统安全	157
9.1 GSM 系统简介	157
9.2 GSM 系统的安全目标和安全实体	159
9.2.1 GSM 系统的安全目标	159
9.2.2 GSM 系统的安全实体	160
9.3 GSM 系统的鉴权机制	161
9.3.1 GSM 系统标识码	161
9.3.2 GSM 系统的鉴权过程	162
9.4 GSM 系统的加密机制	163
9.5 GSM 系统的匿名机制	164
9.6 GSM 系统的安全性分析	164
第 10 章 GPRS 安全	166
10.1 GPRS 简介	166
10.2 GPRS 系统的鉴权	168
10.3 GPRS 系统的加密机制	169
10.4 GPRS 系统的匿名机制	170
10.5 安全性分析	170
第 11 章 窄带 CDMA 安全	171
11.1 CDMA 系统简介	171
11.2 CDMA 系统的鉴权	172
11.2.1 CDMA 系统标识码与安全参数	172



11.2.2 CDMA 系统的鉴权	173
11.3 CDMA 系统的空口加密	176
11.4 CDMA 中的密钥管理	176
11.4.1 A Key 的分配和更新	177
11.4.2 SSD 的更新	177
第 12 章 WCDMA 安全	179
12.1 3G 系统概述	179
12.2 3G 安全结构	180
12.3 认证与密钥协商机制	182
12.3.1 认证与密钥协商协议	182
12.3.2 认证与密钥协商算法	184
12.3.3 AKA 的安全性分析	186
12.4 空中接口安全机制	187
12.4.1 f_8 算法概述	187
12.4.2 f_8 算法的构造方式	188
12.4.3 f_9 算法概述	189
12.4.4 f_9 算法的构造方式	191
12.4.5 KASUMI 算法	192
12.5 核心网安全	197
12.5.1 安全域的划分	198
12.5.2 MAP 安全	198
12.5.3 IPsec 安全	202
12.6 应用层安全	205
12.6.1 WAP 概述	205
12.6.2 WAP 安全	208
12.7 WPKI 介绍	210
12.7.1 WPKI 组成	211
12.7.2 WPKI 中的证书	212
12.7.3 WPKI 的模式	212
第 13 章 数字集群通信系统安全	215
13.1 数字集群系统及其标准简介	215
13.2 TETRA 标准及网络结构	217



13.2.1	TETRA 标准	217
13.2.2	TETRA 系统结构	218
13.2.3	TETRA 标准中定义的接口	219
13.2.4	TETRA 帧结构	220
13.3	TETRA 系统的基本鉴权过程	220
13.3.1	SwMI 对 MS 的单向鉴权	221
13.3.2	MS 对 SwMI 的单向鉴权	222
13.3.3	MS 与 SwMI 的双向鉴权	223
13.4	空中接口加密	226
13.4.1	空中接口加密在 TETRA 中的层次	226
13.4.2	安全类别	226
13.4.3	空中接口加密的主要算法	227
13.4.4	空中接口加密中的密钥	228
13.5	TETRA 系统端到端安全	230
13.5.1	端到端安全的总体架构	230
13.5.2	加密算法	232
13.5.3	语音加密和同步	232
13.5.4	短消息加密	234
13.5.5	密钥管理	235
13.5.6	具体实施的建议	236
第 14 章	无线局域网安全	237
14.1	无线局域网的结构	237
14.2	IEEE 802.11 WEP 的工作原理	239
14.3	针对 WEP 的分析	242
14.4	802.11i 的主要加密机制	245
第 15 章	WiMAX 安全	251
15.1	WiMAX 简介	251
15.1.1	优点	252
15.1.2	协议模型	252
15.2	WiMAX 安全子层	253
15.2.1	IEEE 802.16 固定接入系统的安全机制	253
15.2.2	IEEE 802.16 移动接入系统的安全机制	255



15.2.3 IEEE 802.16-2004 和 IEEE 802.16-2005 的比较	260
第 16 章 移动 Ad Hoc 网络安全	261
16.1 移动 Ad Hoc 网络简介	261
16.1.1 移动 Ad Hoc 网络的特点	262
16.1.2 移动 Ad Hoc 网络的应用领域	263
16.1.3 移动 Ad Hoc 网络的安全弱点	264
16.2 移动 Ad Hoc 网络的密钥管理	265
16.2.1 部分分布的 CA(Partially Distributed CA)	265
16.2.2 自安全方案(Self-Securing)	266
16.3 移动 Ad Hoc 网络的安全路由	267
16.3.1 Ad Hoc 网络路由协议及其分类	267
16.3.2 典型的 Ad Hoc 网络路由协议	269
16.3.3 针对 Ad Hoc 网络路由协议的攻击	271
16.3.4 Ad Hoc 网络安全路由协议	274
第 17 章 蓝牙安全	278
17.1 蓝牙技术简介	278
17.2 蓝牙安全概述	279
17.3 加密	280
17.4 认证	285

第 4 部分 进展篇

第 18 章 移动可信模块	289
18.1 可信计算概念	289
18.1.1 可信计算的历史	289
18.1.2 可信计算的概念	291
18.1.3 可信计算的发展	294
18.2 可信计算平台(TCP)	295
18.2.1 可信计算平台的构成	295
18.2.2 可信计算平台安全体系	298
18.3 移动可信模块(MTM)	299
18.3.1 MTM 介绍	299



18.3.2 MRTM 和 MLTM	300
18.3.3 MTM 中信任链的传递	301
18.4 总结	303
第 19 章 基于 RFID 的移动电子支付安全	304
19.1 概述	304
19.2 RFID 技术	306
19.2.1 RFID 系统组成	307
19.2.2 RFID 技术的基本工作原理	307
19.3 RFID 安全	308
19.3.1 RFID 的安全隐患	308
19.3.2 RFID 安全机制	309
19.4 基于 RFID 的移动电子支付安全	311
19.5 总结	312
第 20 章 传感器网络安全	314
20.1 无线传感器网络概述	314
20.1.1 无线传感器网络的体系结构	314
20.1.2 无线传感器网络的特征	316
20.2 无线传感器网络安全挑战与措施	317
20.2.1 无线传感器网络面临的安全威胁	317
20.2.2 无线传感器网络的安全目标	319
20.2.3 无线传感器网络的安全措施	320
20.3 无线传感器网络的认证机制	322
20.3.1 基于对称密码算法的认证协议	322
20.3.2 基于公钥密码算法的认证协议	325
20.4 无线传感器网络中的加密技术	326
20.5 无线传感器网络的密钥管理	328
20.5.1 WSN 密钥管理要求及分类	328
20.5.2 典型 WSN 密钥管理方案	330
20.6 总结	332
第 21 章 移动版权保护	333
21.1 数字版权管理系统	333
21.1.1 数字版权管理系统分析	333



21.1.2	数字版权管理技术	336
21.1.3	数字版权管理与移动版权保护	338
21.2	OMA DRM 2.0 标准	340
21.2.1	DRM 2.0 技术框架组成	340
21.2.2	OMA DRM 2.0 功能体系结构	341
21.2.3	OMA DRM 2.0 的安全架构	342
21.2.4	OMA DRM 2.0 的内容分发和内容保护	347
21.2.5	OMA DRM 2.0 工作流程	350
21.2.6	OMA DRM 2.0 的信任模型	350
21.2.7	OMA DRM 2.0 和 OMA DRM 1.0 的区别	350
21.3	移动版权保护的发展趋势	352
21.4	总结	353
	参考文献	354

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。

