Broadview
www.broadview.com.cn

无线电安全攻防大揭秘

360独角兽安全团队(UnicornTeam) 杨卿　黄琳　等著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

无线电安全攻防大揭秘

360独角兽安全团队(UnicornTeam) 杨卿　黄琳 等著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书着眼于无线通信安全领域，以无线通信距离由近及远的顺序，讨论各种无线通信系统的安全问题。协议分析结合攻防实例，深入介绍安全攻防技术。案例题材囊括物联网、车联网、移动通信、卫星导航及相关的软硬件安全。本书共分 9 章，其中第 1 章介绍作者在无线安全攻防领域多年来的思路、理念及对该领域未来的展望；第 2~8 章分别介绍各种无线通信系统的安全攻防（RFID、无线遥控、ADS-B、BLE、ZigBee、移动通信、卫星通信等）及实例测试；第 9 章介绍无线安全研究的重要手段，软件无线电工具 GNU Radio 和相关硬件的详细使用。

希望本书可以为对无线通信安全感兴趣的同学、从业者、产品研发人员提供有价值的安全参考。

图书在版编目（CIP）数据

无线电安全攻防大揭秘 / 杨卿等著. —北京：电子工业出版社，2016.5
ISBN 978-7-121-28580-6

Ⅰ. ①无… Ⅱ. ①杨… Ⅲ. ①无线电通信－安全技术－研究 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字（2016）第 076131 号

策划编辑：张春雨
责任编辑：葛　娜
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　　印张：19　　字数：423 千字
版　　次：2016 年 5 月第 1 版
印　　次：2016 年 5 月第 1 次印刷
印　　数：4000 册　　定价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：gena@phei.com.cn。

推荐序 1

本人已从事通信理论的研究与教学工作二十多年，曾承担多项国家级科研项目以及与企业合作开发项目，在通信系统设计、算法优化和协议实现等方面积累了一些经验。

应该讲，所有通信系统都存在安全问题，通信系统安全问题涉及设备安全、内容安全和防护安全等，各种安全措施伴随着通信和网络技术的发展而发展，特别是当今互联网技术的发展引发的安全问题越来越突出。

近年来，国家层面对网络空间安全越来越重视，无线电的安全问题也越来越受到政府、企业和公众的关注。伪基站、非法广播电台，已经真实地影响到普通老百姓的生活。并且，随着软件无线电技术的发展，无线通信协议的实现成本变得越来越低，这意味着攻击的门槛也变得越来越低。在 2009 年，我的学生在研究 OpenBTS 的时候，就已经发现搭建的基站很容易把周围的手机吸入它的网络，这也许是国内最早的伪基站。只是那时，我们从未想到，伪基站会泛滥成如今的样子。

本书作者黄琳是我的学生，一位具有丰富经验的无线通信领域的专家，对无线通信和无线电安全进行了长期深入研究和实践。2010 年，她曾写过一本《GNU Radio 入门》教程，在网络上影响很大。她还曾作为中国 360UnicornTeam 的唯一女性代表在第 23 届 DEFCON 世界黑客大会上发表演讲，在无线电安全领域产生了重要影响。

《无线电安全攻防大揭秘》这本书，涵盖当前常见无线电多种应用的安全问题，内容讲解深入浅出、通俗易懂、可读性强，具备一般专业基础知识的读者均可阅读。本书既适合从事无线电安全领域的技术人员阅读，对无线电安全方面感兴趣的一般读者也可以通过本书对该领域有初步的了解。

王文博（北京邮电大学教授，研究生院常务副院长）

推荐序 2

无线电安全是一个既年轻又古老的领域。有多古老呢？和无线电本身一样古老。

1903 年，当马可尼在伦敦皇家学院公开展示无线电通信时，他的竞争对手马斯基林就劫持了马可尼演示的通信。马斯基林在发射的信号中骂马可尼是“老鼠”、“欺骗公众的意大利佬”，弄得现场非常尴尬。直到今天，信号劫持及其防御，仍然是无线电安全领域的重要内容。

二战期间，盟军成功破解纳粹用 Enigma 机加密的无线电报，大大改变了战局。盟军和纳粹当年在加密解密对抗上所做的工作，今天也仍是无线电安全领域的重要内容。

随着时间的推移，无线电通信技术日趋先进、便捷和普及，无线电安全领域的攻防对抗也逐渐从神秘的实验室，走到了大众的身边。20 世纪 80 年代，使用模拟信号的移动电话“大哥大”在香港流行，市面上也就随之出现了专门用于窃听“大哥大”的“小弟小”（粤语叫“细佬细”）。

进入 21 世纪后，信息技术一日千里，作为其重要组成部分的数字无线电通信技术，也以惊人的速度在发展。然而，人们对这个领域安全对抗的了解却一度没有跟上。十几年前，黑市上刚出现 GSM 窃听装置时，还有不少通信领域的专家出来辟谣，认为 GSM 不可能被窃听。现在，GSM 的不安全，至少在信息安全工作者中已经成为常识。

今天，在智能手机的引领下，万物互联的趋势不可阻挡，也带动了各种无线通信技术的发展。当街边的大爷大妈也能随口说出“WiFi”、“GPS”这些词的时候，当家门口的电表也被接上天线的时候，无线电安全越来越多被大众关注也就不奇怪了。然而，相对软件安全领域，无线电安全人才还是比较缺乏的。

我国每年培养的通信人才并不少，高校的安全专业建设这几年也逐渐跟上来了。但懂通信、会逆向，能拆能焊，又有攻防思维的跨界人才就比较稀罕了。而未来，这个领域会越来越重要。希望这本书能帮助更多对此有兴趣的年轻人走上无线电安全研究之路。

无线传千里，攻防永不眠。

于旸（腾讯玄武实验室总监，网名“tombkeeper”）

推荐序 3

I first meet Yang Qing at Blackhat 2014 and was pleasantly surprised to learn such a young face leads a team on hardware security. Since then he has accomplished several works, ranging from GPS spoofing to designing various gadgets for protecting users' security and privacy. When he told me about their book on wireless security, I was delighted because wireless security is such an important topic and needs much more attention and talents than what we have today.

With the proliferation of wireless technologies, numerous emerging wireless devices have been woven into the fabric of our daily life, ranging from controlling our home appliances to making our vehicles automatically seek for help in emergency situations. Unfortunately, the security on these wireless devices has almost always lagged behind the plethora of the interests in integrating wireless technologies into almost everything. Granted that manufactories and designers have gradually increased their motivation in securing their devices, we have a long way to go. Spreading knowledge on wireless security is one of the critical efforts towards securing wireless devices, and this book serves as a good endeavor along this goal.

Many academic books on wireless communication and wireless security are available, and many of them focus on the theoretical principles. This book is a collection of the systems works that Qing and his team have carried out in the past few years as well as the state of the art. The book covers a wide range of wireless devices, such as RFID, Bluetooth, Zigbee, GPS, and it contains many results, plots, screen-snapshots from real world experiments.

This book can serve as a good tutorial for those who want to have their hand dirty and reproduce the prior findings. It can also be a good reference book for those who want to find out the off-the-shelf tools for exploring the wireless world. I hope this book can help to foster talents in wireless security and to teach them necessary skills to secure the wireless world for many years to come.

徐文渊（浙江大学教授，南卡大学终身教授）

前言

本书的由来

想到在广泛的无线频谱里，有那么多技术应用可以被我们研究，寻找漏洞，并通过漏洞影响一个又一个现实的设备，如手机、电脑、汽车、传感器、工控机、智能家居，甚至是植入在人体内的各种医疗设备，你会不会感到很兴奋呢？是的，这其实就是我及我的团队一直专注的方向和领域。无线电技术是人类能前进到此刻的重大发明之一，我们不能忽视这里面可能发生的安全问题，我期待在未来会有更多的朋友加入一同在这一安全领域遨游。我们团队在国内还将继续作为先驱者带动这个安全领域的健康发展。这也是我们将多年来的所有积累编著成书的原动力。

同时希望本书也可以为对无线通信安全感兴趣的同学、从业者、产品研发人员提供有价值的安全参考。

本书的结构

第 1 章介绍我本人在无线安全攻防领域多年来的思路、理念以及对该领域未来的展望。

第 2~8 章分别介绍无线通信主流技术的安全攻防（RFID、射频、ADS-B、BLE、ZigBee、移动通信网络、卫星通信等）及实例测试。由独角兽安全团队（UnicornTeam）核心成员黄琳、单好奇、张婉桥、李均共同编写。

第 9 章作为无线安全研究实操的核心内容，介绍无线安全研究工具 GNU Radio 的详细使用。本章由《GNU Radio V0.99 入门》作者黄琳基于旧版本更新而来，是不可多得的珍贵教程。

致谢

感谢 360 公司周总、齐总为独角兽团队全体成员提供了自由开心的工作环境与富有竞争力的福利待遇。

感谢 360 公司首席安全官谭晓生对独角兽团队成员工作的指导与栽培。

感谢 360 信息安全部门 0keeTeam 张鲁、VulpeckerTeam 宋申雷、NirvanTeam 高雪峰在工作上的支持与帮助。

感谢 360 人力资源部王文萍、梁丽丽、王娜在工作上的支持与帮助。

感谢 360 公司市场传播部韩笑、尹乃潇、徐粲然、张震宇、马利娜、许传朝、陈晨、苑一时、景义哲、裴智勇、孙红娜等同事对我们团队工作的支持与帮助。

感谢 360 公司李洪亮、张卓、李向东、张睿、郑文斌、张聪、蔡玉光、唐青昊、林伟、刘小雄、赵晋龙等同事在工作上的协助。

感谢 360 独角兽团队黄琳、单好奇、张婉桥、李均、简云定、柴坤哲、郑玉伟、曾颖涛、袁舰、秦明闯、张强、张笔、王佳、郭怡婷、顾为群、徐佳、杨芸菲、王永涛、任兴典、张晓东、唐志红、崔婷等同事的努力付出。

杨卿（360 独角兽安全团队总监）

目录

第 1 章　鸟瞰无线安全攻防 1

1.1　无线安全概述 1

1.1.1　无线安全的由来 1

1.1.2　无线安全与移动安全的区别 2

1.1.3　无线安全的现状 2

1.2　无线安全攻防思路 3

1.2.1　常见攻击对象 3

1.2.2　无线安全攻击手段 3

1.2.3　无线安全防范思路 4

1.2.4　无线安全趋势 4

第 2 章　RFID 智能卡的安全研究 6

2.1　Mifare Classic 智能卡简介 6

2.2　Mifare Classic 智能卡安全分析 7

2.2.1　RFID 芯片硬件逆向分析 8

2.2.2　RFID 芯片加密算法细节 10

2.2.3　Mifare Classic 业界破解过程回顾 12

2.3　Mifare Classic 智能卡破解实例 15

2.3.1　Proxmark III简介 15

2.3.2　Proxmark III固件烧写及使用 17

2.3.3　Proxmark III客户端 20

2.3.4　Proxmark III安全测试 Mifare Classic 用例 23

2.3.5 Chameleon-Mini 简介 29
2.3.6 Chameleon-Mini 固件烧写及使用 30
2.3.7 Proxmark III与 Chameleon-Mini 配合模拟 Mifare Classic 35
2.3.8 RFID 高频攻防总结 36
2.4 低频 ID 卡安全分析 36
2.4.1 低频 ID 卡简介 36
2.4.2 ID 卡编码原理 37
2.4.3 ID 卡译码原理 38
2.4.4 ID 卡数据读取 39
2.4.5 ID 卡卡号格式 40
2.5 低频 ID 卡克隆攻击 41
2.5.1 Proxmark III模拟攻击 42
2.5.2 白卡克隆攻击 43
2.5.3 HackID 模拟攻击 44
2.6 EMV 隐私泄露 45
2.6.1 EMV 简介 45
2.6.2 非接触式芯片卡隐私泄露原理 46
2.6.3 非接触式芯片卡隐私泄露现象 49
2.6.4 非接触式芯片卡个人隐私保护 50

第 3 章 短距离无线遥控系统 52
3.1 遥控信号嗅探与安全分析 52
3.2 遥控信号重放攻击 55
3.3 车库门固定码暴力破解 59
3.3.1 暴力破解的复杂度分析 59
3.3.2 固定码暴力破解的硬件实现 61
3.4 汽车遥控钥匙信号安全分析 64
3.5 汽车胎压传感器系统安全分析 72

第 4 章 航空无线电导航 78
4.1 ADS-B 系统简介 78
4.1.1 ADS-B 是什么 79

4.1.2 1090ES 的含义 79
4.2 ADS-B 信号编码分析 80
4.2.1 调制方式 80
4.2.2 报文格式 81
4.2.3 高度编码 82
4.2.4 CPR 经纬度编码 83
4.2.5 CRC 校验 85
4.3 ADS-B 信号欺骗攻击 85
4.4 攻防分析 87
参考文献 88

第 5 章 蓝牙安全 90
5.1 蓝牙技术简介 90
5.2 蓝牙安全概述 91
5.3 蓝牙嗅探工具 Ubertooth 93
5.3.1 Ubertooth 软件安装 94
5.3.2 使用 Ubertooth 95
5.4 低功耗蓝牙 97
5.4.1 TI BLE Sniffer 97
5.4.2 使用手机应用读写 BLE 设备的属性 101
5.4.3 模拟 BLE 设备发射数据包 102

第 6 章 ZigBee 安全 106
6.1 ZigBee 简介 106
6.1.1 ZigBee 与 IEEE 802.15.4 的关系 107
6.1.2 802.15.4 帧结构 108
6.1.3 ZigBee 的 MAC 帧类型 109
6.1.4 ZigBee 设备类型及网络拓扑 109
6.1.5 ZigBee 组网过程 110
6.1.6 ZigBee 的应用层 112
6.1.7 ZigBee 的应用支持子层 112
6.1.8 ZigBee 应用 Profile 113

6.2 ZigBee 安全 113
6.2.1 安全层次 114
6.2.2 密钥类型 115
6.2.3 安全等级 115
6.2.4 密钥分发 116
6.2.5 ZigBee 节点入网认证 116
6.3 ZigBee 攻击 117
6.3.1 攻击工具介绍 117
6.3.2 协议分析软件 118
6.3.3 网络发现 122
6.3.4 对非加密信息的攻击 124
6.3.5 对加密信息的攻击 126
6.4 攻击实例 131
6.4.1 从设备中获取密钥 131
6.4.2 利用密钥可进行的攻击 138
6.5 攻防分析 141

第 7 章 移动通信网络安全现状 142

7.1 GSM 系统安全现状 142
7.1.1 GSM/UMTS 系统术语和基本概念的简介 142
7.1.2 GSM 加密算法的安全性 146
7.1.3 GSM 攻击 150
7.2 IMSI Catcher 156
7.2.1 什么是 IMSI Catcher 156
7.2.2 GSM 环境下的 IMSI Catcher 157
7.2.3 UMTS 环境下的 IMSI Catcher 159
7.2.4 LTE 环境下的 IMSI Catcher 160
7.2.5 IMSI Catcher 的缺陷 162
7.2.6 Stingray 手机追踪器 163
7.2.7 IMSI Catcher Detector 166
7.3 Femtocell 安全 169
7.3.1 Femtocell 简介 169

7.3.2 家庭基站的攻击面 170
7.3.3 CDMA Femtocell 漏洞综合利用 171
7.3.4 基于 VxWorks 的 GSM Femtocell 流量捕获器 178
7.3.5 350 元玩转 Femto 184
7.4 降级攻击 188
7.5 移动通信网络中的防御措施 189

第 8 章 卫星通信安全 190
8.1 人造卫星概况 190
8.2 GPS 的安全研究 192
8.2.1 GPS 嗅探与安全分析 192
8.2.2 GPS 信号伪造风险评估 195
8.2.3 防御方法及建议 211
8.3 Globalstar 系统的安全分析 212
8.3.1 Globalstar 的码分多址技术 213
8.3.2 Globalstar 数据破解 215
8.3.3 可能的攻击手法 220
参考文献 221

第 9 章 无线安全研究工具——GNU Radio 223
9.1 软件无线电技术 223
9.1.1 SDR 的强大能力 224
9.1.2 SDR 的用途 225
9.2 GNU Radio 简介 226
9.3 GNU Radio 支持的硬件工具 228
9.3.1 USRP 228
9.3.2 RTL-SDR 232
9.3.3 HackRF 236
9.3.4 bladeRF 237
9.4 GNU Radio 安装 239
9.4.1 从源码手动安装 240
9.4.2 使用 PyBOMBS 安装 GNU Radio 243

9.4.3 如何更新软件版本 245
9.5 安装好之后可以做的第一件事 245
9.5.1 如果有硬件 245
9.5.2 如果没有硬件 249
9.6 GNU Radio 的一些基本概念 250
9.6.1 流图（flow graph） 251
9.6.2 信号流中的颗粒（item） 251
9.6.3 采样率 252
9.6.4 metadata 253
9.6.5 传递数据的两种方式：信号流和消息 254
9.7 初学者如何使用 GNU Radio 254
9.7.1 如何编写流图——Python 应用程序 255
9.7.2 如何编写自己的 C++模块 265
9.7.3 如何编写自己的 Python 模块 276
9.7.4 调试代码的方法 279
9.8 范例解读——OFDM Tunnel 283
9.8.1 系统框图和 MAC 帧的构成 285
9.8.2 物理层 286
9.8.3 调试方法 288

第 1 章

鸟瞰无线安全攻防

1.1 无线安全概述

1.1.1 无线安全的由来

“无线”安全是庞大的信息安全体系下一门很广泛的学科。当今社会，电子产品大量依靠各种无线技术，从近场通信 NFC、蓝牙 BLE、射频 RF、工控无线传输 ZigBee、无线局域网 WiFi，到手机蜂窝网络 Cellular、卫星定位 GPS、卫星通信 SATCOM，这些都属于无线技术领域，所以无线通信技术上的传输、认证、加密等安全问题，在各种设备对无线技术依赖加深的情况下变得越来越重要。从现在到未来，人类对这些技术的安全拥有足够的掌控也将是非常必要的。因此，如何正确地使用无线通信技术，并保证其安全，是每一个研发、产品、安全研究人员都要认真思考的问题。

遥想 10 年前，国内安全圈里的黑客们还在最早的无线安全时代（无线局域网、WiFi）研究与徘徊，当时破解 WiFi 密码、蹭网继而进行网络渗透是最传统的无线攻击方法。那个时代，也是无线局域网安全最火热的年代，无线安全研究者们专注于寻找性能优良的无线网卡，搭配自己优化的无线破解平台或使用 BackTrack、Kali 这类完善的环境对自己感兴趣的一个又一个无线热点进行安全评估，体会那种突破无线密码、接入目标无线网络的成就感。

随着无线攻防手段的更新，攻击方法也有了更有趣的发展，如先侦测无线客户端发出的曾经连接过的热点的 Probe 信息，再通过软 AP 程序产生相同名字热点的所谓 EvilAP 的钓鱼攻击方法，将无线目标拉入虚假的无线环境进而发起攻击，或者窃取目标网络流量中的敏感信息。独角兽团队所支持的 2015 年 315 晚会上 WiFi 安全环节的出现，也让圈里的老无线安全研究者的心为之一动。这个安全演示环节出自 DEFCON 黑客大会 Wireless Village 上有名的 The Wall of

Sheep（绵羊墙），这个项目是为了教育人们——“你很可能随时都在被监视”，同时也给那些参会的人难堪，参加安全大会还如此不注意安全，难怪被贴到绵羊墙上。绵羊墙的账号和部分隐匿的密码将被投影在专门的一个会议室内的大屏幕上，The Wall of Sheep 大约由 7 名来自北美的安全人士维护，他们每年花 2 周时间来拉斯维加斯参加 DEFCON。大会提供免费的“hostile”的网络（BlackHat 和 DEFCON 提供的无线网络）供参会者接入访问，如果接入了，那么你的所有网络活动都可能被监听和探测。

1.1.2　无线安全与移动安全的区别

现在安全行业对“无线”及“无线安全”的概念是略模糊的，多数从业者认为无线即指手机无线端，无线安全则指手机系统安全、App 端安全。这其实是不正确的，这个安全领域更应该定义为移动安全。本书所提到的无线安全则是更广义的，是指所有使用无线通信协议的无线电技术的安全，即“无线电安全”。

1.1.3　无线安全的现状

随着手机的普及和人们日益增长的随时随地无线上网的需求，针对 WiFi 的各类攻击屡见不鲜，从国内各类媒体对用户在咖啡厅等公共场所上网被钓鱼事件的报道就可以发现，WiFi 安全已经是一个社会安全问题，手机厂商、安全公司也都对 WiFi 造成用户隐私信息泄露等问题在各自能把控发力的地方下足了工夫。如苹果公司在 iOS 8 系统上增加了新的安全特性，可以使设备的无线 MAC 地址随机化，用来躲避在使用 WiFi 的过程中暴露自己手机的“物理指纹”；安全厂商也在各自的手机卫士类产品内增加了对周围无线热点评估的功能，以谋求提高用户连接 WiFi 时的安全性，使用户不受黑客无线钓鱼攻击的威胁。

那么我们只关注 WiFi 安全就可以了吗？答案是否定的，随着物联网（IoT）的持续蓬勃发展，现在的手机、智能设备对各类无线模块、传感器的需求越来越大，蓝牙、GPS、NFC 模块早已成为必备项。此时此刻，我们从安全的角度来看，整个行业对于使用这些无线技术的安全准备是不足的。

美国 Todd Humphreys 教授领导的无线导航实验室，是 GPS 安全研究领域非常领先的一个团队。早在 2012 年，Todd Humphreys 教授就在 TED 发表了演讲，呼吁公众注意 GPS 安全。在 DEFCON 23 上，中国独角兽团队的安全研究员黄琳向全球展示了如何使用低成本的软件无线电设备欺骗手机、汽车甚至无人机。Todd Humphreys 教授在 2016 年 2 月又以文章 *Lost in Space: How secure is the Future of Mobile Positioning?* 再次提出了他对于未来依赖 GPS 技术的设备在受到