

Inside Radio: An Attack and Defense Guide

Qing Yang · Lin Huang

Inside Radio: An Attack and Defense Guide

Qing Yang
Radio Security Research Department
360 Technology Co. Ltd.
Beijing
China

Lin Huang
Radio Security Research Department
360 Technology Co. Ltd.
Beijing
China

ISBN 978-981-10-8446-1 ISBN 978-981-10-8447-8 (eBook)
<https://doi.org/10.1007/978-981-10-8447-8>

Jointly published with Publishing House of Electronics Industry, Beijing
ISBN: 978-7-121-28580-6 Publishing House of Electronics Industry, Beijing

Library of Congress Control Number: 2018933012

© Publishing House of Electronics Industry, Beijing and Springer Nature Singapore Pte Ltd. 2018

This work is subject to copyright. All rights are reserved by the Publishers, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publishers, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publishers nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publishers remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Foreword I

I have been teaching and studying communication theory for more than 20 years and have undertaken multiple scientific research projects on the national level. By cooperating with enterprises in development projects, I accumulated some experience in communication system design, algorithm optimization, and protocol implementation.

It can be said that all communication systems have security problems. The security of communication systems includes device security, content security, and defense. With the advancement of communication and network technologies, various security measures have been developed and updated. However, the development of Internet technology has caused a lot of security concerns.

In recent years, the government is paying more and more attention to network security, and wireless security has attracted the interest of the government, enterprises, and the public. Fake base stations and illegal broadcasting stations are influencing the daily lives of ordinary people. Moreover, with the development of SDR technology, wireless communication protocols can be implemented at a lower cost, and the threshold of attack was lowered. In 2009, my students found during their study of OpenBTS that the base stations set up by themselves can easily attract cell phones into their network. Those base stations may be the first fake ones in China. However, we failed to forecast that such 2G fake base stations can be so common and bring big risk to people today.

Lin HUANG, the author of this book is my student and an expert with rich experience in wireless communication. She has been doing research in wireless communication and wireless security for a long time. In 2010, she wrote a tutorial entitled Introduction to GNU Radio, which had a huge impact in Chinese SDR field. She also delivered a speech in the DEFCON 23 as the only female representative from China.

This book has covered the security problems of many common wireless applications. It provides in-depth, readable, and easy-to-understand knowledge on wireless communication. You can easily read and comprehend this book even if you only know the basics of wireless technology. This book is very suitable for technicians working in wireless security field, and it may help general readers gain a basic understanding of wireless security as well.

Wenbo Wang

Professor of Beijing University of Posts and Telecommunications
Vice President of Beijing University of Posts and Telecommunications

Foreword II

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 of 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 toward 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, and GPS, and it contains many results, plots, and 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.

Wenyuan Xu
Professor of Zhejiang University
Associate Professor of University of South Carolina

Foreword III

Wireless security is both a new and old field. Actually, it is as old as wireless technology itself.

When Marconi was demonstrating wireless communication in Imperial College London in 1903, his competitor Maskelyne hijacked his communication and addressed Marconi as a “mouse” and “Italian con artist” in the transmitted signals. This incident embarrassed the entire demonstration. Until now, signal hijacking and its defense are still an important part of wireless security.

During WWII, the allies successfully cracked the wireless telegraphy of the Nazis encrypted by “Enigma” and changed the war situation. What the allies and Nazis did in the combat of encryption and decryption is exactly what we learn in the field of wireless security today.

With time, wireless communication technology is becoming more and more advanced, convenient, and popular, and wireless attack and defense have come out of the lab and entered our daily lives. In the 1980s, analog mobile phones became popular in Hong Kong. And soon afterward, an eavesdropping device named “Small Brother” emerged in the market.

In the twenty-first century, digital communication is advancing in a rapid speed as part of information technology. However, people’s understanding of digital security is not developing at the same pace. More than a decade ago, when GSM eavesdropping devices appeared in the black market, many telecommunication experts remarked that GSM could not be eavesdropped. However, the insecurity of GSM has become the common sense among information security professionals today.

Nowadays, as smartphones are leading the trend of the Internet of Things, wireless communication technologies are also developing steadily. When even old people are using the words “WiFi” and “GPS” in their daily life, and electricity meters outside our doors become wireless devices, it is not surprising that common people are paying more and more attention to wireless security. However, compared to the software security field, there is a lack of sufficient talents in wireless security.

There are many telecommunication talents, and security disciplines in colleges are gradually catching up with the technological trend. However, experts experienced in telecommunication, reverse engineering hands-on practice and attack and defense methods all at the same time are still urgently needed. And the wireless security field will become even more important in future. I hope this book will encourage more young people interested in wireless security research to set foot in this field.

Wireless communication spreads across borders, and security never leaves our lenses.

Yang Yu
Director of Xuanwu Lab of Tencent

Preface

Radio waves widely exist around us, although you cannot see them. There are various kinds of systems using wireless connections. We focus on the vulnerabilities in these wireless connections and find that the vulnerabilities can affect the devices such as cell phones, computers, cars, sensors, industrial computers, smart home devices, and even various medical devices that are implanted in the human body. This is actually also the main direction and focus UnicornTeam have been working on.

Radio technology is becoming more and more important in the times of Internet of Things ahead. We cannot ignore the security issues that may occur. We wish more people join in the community of security in the future. Our team will continue as a pioneer to promote the development of the community in communication security. With this in mind, we wrote this book which summarizes our research results over the recent years. The content of the book covers the fundamentals as well as our practices in industry which would be beneficial to many readers in spite of their knowledge backgrounds. At the same time, we hope this book can provide a valuable reference for students, security practitioners, and product developers who are interested in wireless communication security.

The structure of this book is as follows:

Chapter 1 gives the overview, ideas, and prospects of the attack and defense in the field of wireless security.

Chapter 2 introduces the detailed usage guide of wireless security research tools: some SDR hardware boards and GNU Radio software. This chapter is a good tutorial for SDR beginners.

Chapters 3–9 are about the security issues in various kinds of wireless system: RFID/NFC, short distance 433/315MHz communication, ADS-B, BLE, ZigBee, cellular network, satellite communication, etc.

Beijing, China
January 2018

Qing Yang
Lin Huang

Acknowledgements

This book is a joint effort by the entire UnicornTeam. The major contributors include:

Qing Yang
Lin Huang
Qiren Gu
Wanqiao Zhang
Haoqi Shan
Jun Li
Yingtao Zeng

In addition, we would like to express our deep appreciation to the researchers who give us permission to share their research results in this book:

Colby Moore
Samy Kamkar
@CrazyDaneHacker
@cnxsoft
@gareth__
@marcnewlin
@z4ziggy,

to the colleagues in 360 Technology, to friends in security communities, and others who gave us support during writing this book, thank you all.

UnicornTeam of 360 Technology

Contents

1	Overview of Wireless Security, Attack and Defense	1
1.1	Overview of Wireless Security	1
1.1.1	Origin of Wireless Security	1
1.1.2	Difference Between Wireless Security and Mobile Security	2
1.1.3	Status Quo of Wireless Security	2
1.2	Wireless Attack and Defense Methods	3
1.2.1	Common Attack Targets	3
1.2.2	Wireless Attack Methods	4
1.2.3	Wireless Defense Methods	5
1.2.4	Trend of Wireless Security	5
2	Tools for Wireless Security Research	7
2.1	Software-Defined Radio Technology	7
2.1.1	SDR Capabilities	8
2.1.2	SDR Usage	9
2.2	SDR Hardware Tools	10
2.2.1	USRP	10
2.2.2	RTL-SDR	12
2.2.3	HackRF	23
2.2.4	BladeRF	25
2.2.5	SDR Software Tool—GNU Radio	37
2.2.6	GNU Radio Installation	38
2.2.7	The First Thing to Do After Installation	45
2.2.8	Example: OFDM Tunnel	50
2.2.9	Sniff Mouse and Keyboard Data	57
	Further Reading	70

3	RFID/NFC Security	71
3.1	Introduction to Mifare Classic	72
3.2	Security Analysis of Mifare Classic	73
3.2.1	Review of the Process of Cracking Mifare Classic	73
3.3	A Real Case of Cracking Mifare Classic	76
3.3.1	Introduction to Proxmark III	76
3.3.2	Burn and Use Proxmark III Firmware	77
3.3.3	Proxmark III Client	82
3.3.4	Test the Security of Mifare Classic with Proxmark III	84
3.3.5	Introduction to Chameleon-Mini	90
3.3.6	Burn and Use Chameleon-Mini Firmware	92
3.3.7	Simulate Mifare Classic by Combining Proxmark III and Chameleon-Mini	95
3.3.8	Conclusion of HF Attack and Defense	98
3.4	Security Analysis of LFID Cards	98
3.4.1	Introduction to LFID Cards	98
3.4.2	Coding Principle of ID Cards	100
3.4.3	Decoding Principle of ID Cards	100
3.4.4	Read Data from ID Cards	101
3.4.5	Format of the ID Card Number	102
3.5	Clone an LFID Card	103
3.5.1	Simulation Attacks with Proxmark III	104
3.5.2	Clone Attacks with a Blank Card	106
3.5.3	Simulation Attacks with HackID	107
3.6	EMV Privacy Leakage	108
3.6.1	EMV Introduction	108
3.6.2	Mechanism of Privacy Leakage in Contactless Chip Cards	109
3.6.3	Phenomenon of Privacy Leakage in Contactless Chip Cards	113
3.6.4	Contactless Chip Card Fraud	114
3.6.5	Privacy Protection in the Use of Contactless Chip Cards	118
	Further Reading	121
4	433/315 MHz Communication	123
4.1	Sniff and Analyze the Security of Remote Control Signals	123
4.2	Attacks by Replaying Remote Control Signals	125
4.2.1	Parking Bar Signal Replay	125
4.2.2	Wireless Door Bell Signal Replay	130
4.2.3	Vibrator Signal Replay	133

4.3	Crack Fixed-Code Garage Doors with Brute Force	143
4.3.1	Complexity of Brute-Force Attack	143
4.3.2	Hardware for Fixed-Code Brute-Force Attack	146
4.4	Security Analysis of Remote Car Key Signals	147
4.4.1	Generation of Remote Control Signals	151
4.4.2	Security Analysis of Keeloq Key Generation Algorithm	154
4.4.3	An Example of Remote Controller Bugs	157
4.4.4	Rolljam Replay Attacks on Car Keys	161
4.5	Security Analysis of the PKE System	162
4.6	Security Analysis of the Tire Pressure Monitoring System	165
	Further Reading	171
5	Aeronautical Radio Navigation	173
5.1	Introduction to ADS-B System	173
5.1.1	Definition of ADS-B	174
5.1.2	Definition of 1090ES	175
5.2	ADS-B Signal Encoding	175
5.2.1	Modulation Method	176
5.2.2	Format of Message	176
5.2.3	Altitude Code	178
5.2.4	CPR Longitude and Latitude Code	178
5.2.5	CRC Validation	180
5.3	ADS-B Signal Sniffing	181
5.3.1	Receive ADS-B Signal with “Dump1090”	181
5.3.2	Receive ADS-B Signal with “gr-air-modes”	183
5.4	ADS-B Signal Deception	187
5.5	Analysis of Attack and Defense	188
	Further Reading	193
6	Bluetooth Security	195
6.1	Introduction to Bluetooth Technology	195
6.2	Bluetooth Sniffing Tool Ubertooth	198
6.2.1	Ubertooth Software Installation	198
6.2.2	Ubertooth Usage	203
6.3	Low-Power Bluetooth	212
6.3.1	TI’s BLE Sniffer	213
6.3.2	Sniff BTLE Data Packets with “Ubertooth-Btle”	216
6.3.3	Read and Write BLE Devices’ Properties with a Mobile App	220
6.3.4	Transmit Data Packets by Simulating the BLE Device	222
	Further Reading	226

7	ZigBee Technology	227
7.1	Introduction to ZigBee	227
7.1.1	The Relationship Between ZigBee and IEEE 802.15.4	228
7.1.2	Structure of 802.15.4 Frames	228
7.1.3	Different Types of MAC Frame in ZigBee	230
7.1.4	Device Types and Network Topology of ZigBee	230
7.1.5	ZigBee Networking	232
7.1.6	Application Layer of ZigBee	232
7.1.7	The Application Support Sub-layer of ZigBee	233
7.1.8	Application Profile of ZigBee	234
7.2	ZigBee Security	234
7.2.1	Security Layers	235
7.2.2	Key Types	236
7.2.3	Security Levels	237
7.2.4	Key Distribution	238
7.2.5	Access Authentication for ZigBee Nodes	239
7.3	ZigBee Attacks	239
7.3.1	Attacking Tools	239
7.3.2	Protocol Analysis Software	241
7.3.3	Network Discovery	243
7.3.4	Attack an Unencrypted Network	245
7.3.5	Attack an Encrypted Network	250
7.4	An Example of Attacking	252
7.4.1	Obtain the Key from the Device	253
7.4.2	Attacks by Using the Key	257
7.5	Summary of Attacks and Defenses	265
	Further Reading	265
8	Mobile Network Security	267
8.1	Security Status of the GSM System	267
8.1.1	Terminology and Basic Concepts of the GSM/UMTS System	267
8.1.2	Security of GSM Encryption Algorithms	271
8.1.3	Active Attack and Passive Attack in GSM	274
8.1.4	GSM Sniffing with “gr-gsm”	280
8.2	IMSI Catcher	298
8.2.1	What Is an IMSI Catcher?	298
8.2.2	IMSI Catcher in GSM Environment	299
8.2.3	IMSI Catcher in UMTS Environment	301
8.2.4	IMSI Catcher in LTE Environment	303

8.2.5	Defect of the IMSI Catcher	308
8.2.6	Stingray Cellphone Tracker	309
8.2.7	IMSI Catcher Detector	311
8.3	Femtocell Security	314
8.3.1	Introduction to Femtocell	314
8.3.2	Attack Surface of Femtocell	315
8.3.3	GSM Femtocell Based on VxWorks	316
8.4	LTE Redirection and Downgrade Attack	321
8.4.1	Redirection Attack Principles	322
8.4.2	The Cause of Redirection Bugs	328
8.5	‘Ghost Telephonist’ Attack	330
8.5.1	Vulnerability Principle	333
8.5.2	Experiment Setting	335
8.5.3	Attack Methods	336
8.5.4	Countermeasures	340
8.6	Analysis of Attack and Defense	342
	Further Reading	342
9	Satellite Communication	343
9.1	Overview of Artificial Satellites	343
9.2	GPS Security Research	344
9.2.1	GPS Sniffing and Security Analysis	344
9.2.2	GPS Spoofing	346
9.2.3	Methods of Defense and Suggestions	358
9.3	Security Analysis of Globalstar System	361
9.3.1	Globalstar’s CDMA Technology	362
9.3.2	Globalstar Data Cracking	363
9.3.3	Possible Attack Methods	367
	Further Reading	368