Inside Radio: An Attack and Defense Guide

Qing Yang · Lin Huang

Inside Radio: An Attack and Defense Guide

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Springer

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

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 — Qing Yang
January 2018 — 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