

The IoT Hacker's Handbook

**A Practical Guide to Hacking
the Internet of Things**

Aditya Gupta

Apress®

The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things

Aditya Gupta
Walnut, CA, USA

ISBN-13 (pbk): 978-1-4842-4299-5
<https://doi.org/10.1007/978-1-4842-4300-8>

ISBN-13 (electronic): 978-1-4842-4300-8

Copyright © 2019 by Aditya Gupta

This work is subject to copyright. All rights are reserved by the Publisher, 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.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Natalie Pao
Development Editor: James Markham
Coordinating Editor: Jessica Vakili

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit <http://www.apress.com/rights-permissions>.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-4299-5. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

Table of Contents

- About the Authorxi**
- About the Technical Reviewerxiii**
- Acknowledgmentsxv**
- Introductionxvii**

- Chapter 1: Internet of Things: A Primer..... 1**
 - Previous IoT Security Issues 4
 - Nest Thermostat 4
 - Philips Smart Home 5
 - Lifx Smart Bulb 6
 - The Jeep Hack 7
 - Belkin Wemo 8
 - Insulin Pump 9
 - Smart Door Locks 9
 - Hacking Smart Guns and Rifles 10
 - Fragmentation in the Internet of Things 11
 - Reasons for IoT Security Vulnerabilities 14
 - Lack of Security Awareness Among Developers 15
 - Lack of a Macro Perspective 15
 - Supply-Chain-Based Security Issues 15
 - Usage of Insecure Frameworks and Third-Party Libraries 16
 - Conclusion 16

TABLE OF CONTENTS

- Chapter 2: Performing an IoT Pentest.....17**
- What Is an IoT Penetration Test? 17
- Attack Surface Mapping..... 19
- How to Perform Attack Surface Mapping..... 19
 - Embedded Devices 20
 - Firmware, Software, and Applications 22
 - Radio Communications..... 26
 - Creating an Attack Surface Map..... 28
- Structuring the Pentest..... 33
 - Client Engagement and Initial Discussion Call 34
 - Additional Technical Discussion and Briefing Call 34
 - Attacker Simulated Exploitation 35
 - Remediation 36
 - Reassessment 36
- Conclusion 37
 - Action Point 37
- Chapter 3: Analyzing Hardware39**
- External Inspection 40
 - Working with a Real Device..... 41
 - Finding Input and Output Ports..... 42
- Internal Inspection..... 45
 - Analyzing Data Sheets..... 51
 - What Is FCC ID 52
 - Component Package..... 56
- Radio Chipsets 57
- Conclusion 58

Chapter 4: UART Communication	59
Serial Communication.....	60
The What, Why, and How of UART	62
UART Data Packet	62
Type of UART Ports	64
Baud Rate.....	65
Connections for UART Exploitation.....	66
Identifying UART Pinouts	70
Introduction to Attify Badge.....	73
Making Final Connections	75
Identifying Baud Rate	76
Interacting with the Device.....	77
Conclusion	80
Chapter 5: Exploitation Using I²C and SPI	81
I ² C (Inter-Integrated Circuit)	82
Why Not SPI or UART	82
Serial Peripheral Interface	83
Understanding EEPROM	83
Exploiting I ² C Security	86
Making Connections for I ² C Exploitation with the Attify Badge.....	88
Understanding the Code	89
Digging Deep into SPI	92
How SPI Works	94
Reading and Writing from SPI EEPROM	94
Dumping Firmware Using SPI and Attify Badge	103
Conclusion	106

TABLE OF CONTENTS

- Chapter 6: JTAG Debugging and Exploitation109**
 - Boundary Scan..... 110
 - Test Access Port..... 112
 - Boundary Scan Instructions 113
 - Test Process 113
 - Debugging with JTAG..... 114
 - Identifying JTAG Pinouts 115
 - Using JTAGulator 117
 - Using Arduino Flashed with JTAGEnum..... 119
 - OpenOCD..... 122
 - Installing Software for JTAG Debugging..... 122
 - Hardware for JTAG Debugging 123
 - Setting Things up for JTAG Debugging..... 125
 - Performing JTAG Exploitation..... 129
 - Writing Data and Firmware to a Device..... 129
 - Dumping Data and Firmware from the Device 131
 - Reading Data from the Device..... 131
 - Debugging over JTAG with GDB..... 132
 - Conclusion 138
- Chapter 7: Firmware Reverse Engineering and Exploitation139**
 - Tools Required for Firmware Exploitation 140
 - Understanding Firmware 140
 - How to Get Firmware Binary 142
 - Extracting Firmware 144

Firmware Internals.....	151
Hard-Coded Secrets	152
Encrypted Firmware.....	156
Emulating a Firmware Binary	162
Emulating an Entire Firmware	166
Backdooring Firmware.....	171
Creating a Backdoor and Compiling It to Run on MIPS-Based Architecture	173
Modifying Entries and Placing the Backdoor in a Location so It Could Be Started Automatically at Bootup.....	178
Running Automated Firmware Scanning Tools	183
Conclusion	185
Chapter 8: Exploiting Mobile, Web, and Network for IoT	187
Mobile Application Vulnerabilities in IoT	188
Inside an Android Application.....	188
Reversing an Android Application	189
Hard-Coded Sensitive Values	194
Digging Deep in the Mobile App	195
Reversing Encryption	202
Network-Based Exploitation	206
Web Application Security for IoT	210
Assessing Web Interface	210
Exploiting Command Injection	213
Firmware Diffing.....	219
Conclusion	222

TABLE OF CONTENTS

Chapter 9: Software Defined Radio.....223

- Hardware and Software Required for SDR..... 224
- Software Defined Radio 225
- Setting Up the Lab 225
 - Installing Software for SDR Research 226
- SDR 101: What You Need to Know..... 227
 - Amplitude Modulation 228
 - Frequency Modulation..... 229
 - Phase Modulation 230
- Common Terminology 231
 - Transmitter 231
 - Analog-to-Digital Converter..... 231
 - Sample Rate 231
 - Fast Fourier Transform 232
 - Bandwidth 232
 - Wavelength..... 232
 - Frequency..... 233
 - Antenna 235
 - Gain 235
 - Filters 237
- GNURadio for Radio Signal Processing 237
 - Working with GNURadio 238
- Identifying the Frequency of a Target..... 249
- Analyzing the Data 252
 - Analyzing Using RTL_433 and Replay 253

Using GNURadio to Decode Data..... 255

Replaying Radio Packets..... 261

Conclusion 263

Chapter 10: Exploiting ZigBee and BLE.....265

 ZigBee 101 265

 Understanding ZigBee Communication 267

 Hardware for ZigBee..... 268

 ZigBee Security 269

 Bluetooth Low Energy 282

 BLE Internals and Association 282

 Interacting with BLE Devices..... 287

 Exploiting a Smart Bulb Using BLE 296

 Sniffing BLE Packets 297

 Exploiting a BLE Smart Lock..... 305

 Replaying BLE Packets 306

 Conclusion..... 308

Index.....311

About the Author

Aditya Gupta is the founder and CEO of Attify, Inc., a specialized security firm offering IoT penetration testing and security training on IoT exploitation. Over the past couple of years, Aditya has performed in-depth research on the security of these devices including smart homes, medical devices, ICS and SCADA systems. He has also spoken at numerous international security conferences, teaching people about the insecurity in these platforms and how they can be exploited. Aditya is also the co-author of the *IoT Pentesting Cookbook* and the author of *Learning Pentesting for Android Devices*.

About the Technical Reviewer

Adeel Javed is an intelligent automation consultant, an author, and a speaker. He helps organizations automate work using business process management (BPM), robotic process automation (RPA), business rules management (BRM), and integration platforms.

He loves exploring new technologies and writing about them. He published his first book, *Building Arduino Projects for the Internet of Things*, with Apress back in 2015. He shares his thoughts on various technology trends on his personal blog (adeeljaved.com).

Acknowledgments

This book could never have been finished without my amazing team at Attify, who poured in their day and night to make sure that we produced quality content as a team.

Introduction

The ten chapters of this book cover a number of topics, ranging from hardware and embedded exploitation, to firmware exploitation, to radio communication, including BLE and ZigBee exploitation.

For me, writing this book was an exciting and adventurous journey, sharing my experiences and the various things I have learned in my professional career and pouring everything into these ten chapters.

I hope you can make the most out of this book and I would highly encourage you to take all the skill sets learned in this book and apply them to real-world problems and help make the Internet of Things (IoT) ecosystem more secure. It is individual contributions that will help us create a safer and more secure world, and you reading this book can play a part in that.

No one is perfect, and this book is bound to have a minor error or two. If you encounter any of those mistakes, let me know and I would be happy to correct them in future editions of *The IoT Hacker's Handbook*.

I also teach three-day and five-day training classes on offensive IoT exploitation, which I would encourage you to attend to get hands-on experience with everything covered in the book. For more information about the online training and live classes, feel free to check out attify-store.com.

The last and the most important part is community! For you, the reader, I want you to be willing enough to share your knowledge with your peers or even with someone who is new to this field. This is how we, as a community, will grow.

INTRODUCTION

That is all from my end. Again, thanks for reading *The IoT Hacker's Handbook* and I wish you all the best for your IoT exploitation endeavors.

Aditya Gupta (@adi1391)
Founder and Chief Hacker,
Attify