

# **PRACTICAL IOT HACKING**

**The Definitive Guide to  
Attacking the  
Internet of Things**

**by Fotios Chantzis, Ioannis Stais,  
Paulino Calderon, Evangelos  
Deirmentzoglou, and Beau Woods**



**no starch  
press**

San Francisco

**PRACTICAL IOT HACKING.** Copyright © 2021 by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13: 978-1-7185-0090-7 (print)

ISBN-13: 978-1-7185-0091-4 (ebook)

Publisher: William Pollock  
Executive Editor: Barbara Yien  
Production Editor: Dapinder Dosanjh  
Developmental Editor: Frances Saux  
Cover Illustration: Rick Reese  
Interior Design: Octopod Studios  
Technical Reviewer: Aaron Guzman  
Copyeditor: Anne Marie Walker  
Compositor: Jeff Wilson, Happenstance Type-O-Rama  
Proofreader: Elizabeth Littrell  
Indexer: BIM Creatives, LLC

**FSC LOGO**  
**FPO**

For information on book distributors or translations, please contact No Starch Press, Inc. directly:  
No Starch Press, Inc.  
245 8th Street, San Francisco, CA 94103  
phone: 1-415-863-9900; info@nostarch.com  
www.nostarch.com

*Library of Congress Cataloging-in-Publication Data*

Names: Chantzis, Fotios, author. | Stais, Ioannis, author. | Calderon, Paulino, author. | Deirmentzoglou, Evangelos, author. | Woods, Beau, author.

Title: Practical IoT hacking : the definitive guide to attacking the internet of things / Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods.

Description: San Francisco : No Starch Press, Inc., 2020. | Includes index.

Identifiers: LCCN 2020029866 (print) | LCCN 2020029867 (ebook) | ISBN 9781718500907 | ISBN 9781718500914 (ebook)

Subjects: LCSH: Internet of things--Security measures. | Penetration testing (Computer security)

Classification: LCC TK5105.8857 .C533 2020 (print) | LCC TK5105.8857 (ebook) | DDC 005.8/7--dc23

LC record available at <https://lcn.loc.gov/2020029866>

LC ebook record available at <https://lcn.loc.gov/2020029867>

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the authors nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

Dedicated to Klajdi and Miranta.

.....

## About the Authors

**Fotios (Fotis) Chantzis** ([@ithilgore](#)) is laying the foundation for a safe and secure Artificial General Intelligence (AGI) at OpenAI. Previously, he worked as a principal information security engineer at Mayo Clinic, where he managed and conducted technical security assessments on medical devices, clinical support systems, and critical healthcare infrastructure. He has been a member of the core Nmap development team since 2009, when he wrote Ncrack under the mentorship of Gordon “Fyodor” Lyon, the original author of Nmap, during the Google Summer of Code. He later worked as a mentor for the Nmap project during the Google Summer of Code 2016 and 2017 and has authored a video course about Nmap. His research on network security includes exploiting the TCP Persist Timer (you can find his paper on the topic published in Phrack #66) and inventing a stealthy port scanning attack by abusing XMPP. Fotis has presented at notable security conferences, including DEF CON. Highlights of his work can be found at his site <https://sock-raw.org/>.

**Ioannis Stais** ([@Einstais](#)) is a senior IT security researcher and head of red teaming at CENSUS S.A., a company that offers specialized cybersecurity services to customers worldwide. Ioannis has participated in more than 100 security assessment projects, including the assessment of communication protocols, web and mobile banking services, NFC payment systems, ATMs and point-of-sale systems, critical medical appliances, and MDM solutions. He holds a master’s degree in computer systems technology from the University of Athens. His research currently focuses on the development of machine learning algorithms for improving vulnerability research, the enhancement of fuzzing frameworks, and an exploration of the current threats in mobile and web applications. He has presented his research at security conferences such as Black Hat Europe, Troopers NGI, and Security BSides Athens.

## About the Co-Authors

**Paulino Calderon** ([@calderpwn](#)) is a published author and international speaker with over 12 years of experience in network and application security. When he isn’t traveling to security conferences or consulting for Fortune 500 companies with Websec, a company he co-founded in 2011, he spends peaceful days enjoying the beach in Cozumel, Mexico. He loves open source software and has contributed to many projects, including Nmap, Metasploit, OWASP Mobile Security Testing Guide (MSTG), OWASP Juice Shop, and OWASP IoT Goat.

**Evangelos Deirmentzoglou** ([@edeirme](#)) is an information security professional interested in solving security problems at scale. He led and structured the cybersecurity capability of the financial tech startup Revolut. A member of the open source community since 2015, he has made multiple contributions to Nmap and Ncrack. He is currently researching a cybersecurity PhD focusing on source code analysis, which he has previously applied for many major US technology vendors, Fortune 500 companies, and financial and medical institutions.

**Beau Woods** ([@beauwoods](#)) is a cyber safety innovation fellow with the Atlantic Council and a leader with the I Am The Cavalry grassroots initiative. He is also the founder and CEO of Stratigos Security and sits on the board of several nonprofits. In his work, which bridges the gap between the security research and public policy communities, he ensures that any connected technology able to impact human safety is worthy of our trust. He formerly served as an entrepreneur in residence with the US FDA and a managing principal consultant at Dell SecureWorks. He has spent the past several years consulting with the energy, healthcare, automotive, aviation, rail, and IoT industries, as well as with cybersecurity researchers, US and international policymakers, and the White House. Beau is a published author and frequent public speaker.

## About the Technical Reviewer

**Aaron Guzman** is co-author of the IoT Penetration Testing Cookbook and a technical leader for Cisco Meraki's security team. As part of OWASP's IoT and Embedded Application Security projects, he leads open source initiatives that raise awareness of IoT security defensive strategies and lower the barrier for entry into IoT hacking. Aaron is co-chair of Cloud Security Alliance's IoT Working Group and a technical reviewer for several IoT security books. He has extensive public speaking experience, delivering conference presentations, trainings, and workshops globally. Follow Aaron's research on Twitter at [@scriptingxss](#).

# BRIEF CONTENTS

Foreword . . . . .	xix
Acknowledgments . . . . .	xxi
Introduction . . . . .	xxiii

## **PART I :THE IOT THREAT LANDSCAPE . . . . . 1**

Chapter 1: The IoT Security World . . . . .	3
Chapter 2: Threat Modeling . . . . .	17
Chapter 3: A Security Testing Methodology . . . . .	35

## **PART II: NETWORK HACKING . . . . . 57**

Chapter 4: Network Assessments . . . . .	59
Chapter 5: Analyzing Network Protocols . . . . .	89
Chapter 6: Exploiting Zero-Configuration Networking . . . . .	117

## **PART III: HARDWARE HACKING. . . . . 155**

Chapter 7: UART, JTAG, and SWD Exploitation . . . . .	157
Chapter 8: SPI and I <sup>2</sup> C . . . . .	189
Chapter 9: Firmware Hacking . . . . .	207

## **PART IV: RADIO HACKING . . . . . 237**

Chapter 10: Short Range Radio: Abusing RFID . . . . .	239
Chapter 11: Bluetooth Low Energy . . . . .	269
Chapter 12: Medium Range Radio: Hacking Wi-Fi. . . . .	287
Chapter 13: Long Range Radio: LPWAN . . . . .	307

**PART V: TARGETING THE IOT ECOSYSTEM . . . . . 333**

Chapter 14: Attacking Mobile Applications. . . . . 335

Chapter 15: Hacking the Smart Home . . . . . 371

Appendix: Tools for IoT Hacking . . . . . 401

Index . . . . . 415



# CONTENTS IN DETAIL

<b>FOREWORD BY DAVE KENNEDY</b>	<b>xix</b>
---------------------------------	------------

<b>ACKNOWLEDGMENTS</b>	<b>xxi</b>
------------------------	------------

<b>INTRODUCTION</b>	<b>xxiii</b>
---------------------	--------------

This Book's Approach . . . . .	xxiv
Who This Book Is For . . . . .	xxiv
Kali Linux . . . . .	xxv
How This Book Is Organized . . . . .	xxv
Contact . . . . .	xxvii

## **PART I: THE IOT THREAT LANDSCAPE** **1**

<b>1</b>	
<b>THE IOT SECURITY WORLD</b>	<b>3</b>

Why Is IoT Security Important? . . . . .	4
How Is IoT Security Different than Traditional IT Security? . . . . .	5
What's Special About IoT Hacking? . . . . .	6
Frameworks, Standards, and Guides . . . . .	8
Case Study: Finding, Reporting, and Disclosing an IoT Security Issue . . . . .	11
Expert Perspectives: Navigating the IoT Landscape . . . . .	12
IoT Hacking Laws . . . . .	12
The Role of Government in IoT Security . . . . .	14
Patient Perspectives on Medical Device Security . . . . .	14
Conclusion . . . . .	16

<b>2</b>	
<b>THREAT MODELING</b>	<b>17</b>

Threat Modeling for IoT . . . . .	18
Following a Framework for Threat Modeling . . . . .	18
Identifying the Architecture . . . . .	19
Breaking the Architecture into Components . . . . .	20
Identifying Threats . . . . .	21
Using Attack Trees to Uncover Threats . . . . .	28
Rating Threats with the DREAD Classification Scheme . . . . .	29
Other Types of Threat Modeling, Frameworks, and Tools . . . . .	30

Common IoT Threats . . . . .	31
Signal Jamming Attacks . . . . .	31
Replay Attacks . . . . .	31
Settings Tampering Attacks . . . . .	32
Hardware Integrity Attacks . . . . .	32
Node Cloning . . . . .	32
Security and Privacy Breaches . . . . .	32
User Security Awareness . . . . .	32
Conclusion . . . . .	33

### 3

## **A SECURITY TESTING METHODOLOGY 35**

Passive Reconnaissance . . . . .	37
The Physical or Hardware Layer . . . . .	40
Peripheral Interfaces . . . . .	40
Boot Environment . . . . .	41
Locks . . . . .	41
Tamper Protection and Detection . . . . .	41
Firmware . . . . .	42
Debug Interfaces . . . . .	42
Physical Robustness . . . . .	42
The Network Layer . . . . .	43
Reconnaissance . . . . .	43
Network Protocol and Service Attacks . . . . .	45
Wireless Protocol Testing . . . . .	47
Web Application Assessment . . . . .	48
Application Mapping . . . . .	48
Client-Side Controls . . . . .	48
Authentication . . . . .	49
Session Management . . . . .	49
Access Controls and Authorization . . . . .	49
Input Validation . . . . .	50
Logic Flaws . . . . .	50
Application Server . . . . .	50
Host Configuration Review . . . . .	50
User Accounts . . . . .	51
Password Strength . . . . .	51
Account Privileges . . . . .	51
Patch Levels . . . . .	52
Remote Maintenance . . . . .	53
Filesystem Access Controls . . . . .	53
Data Encryption . . . . .	53
Server Misconfiguration . . . . .	54
Mobile Application and Cloud Testing . . . . .	54
Conclusion . . . . .	55

**4****NETWORK ASSESSMENTS****59**

Hopping into the IoT Network . . . . .	60
VLANs and Network Switches . . . . .	60
Switch Spoofing . . . . .	61
Double Tagging . . . . .	63
Imitating VoIP Devices . . . . .	65
Identifying IoT Devices on the Network . . . . .	67
Uncovering Passwords by Fingerprinting Services . . . . .	67
Writing New Nmap Service Probes . . . . .	71
Attacking MQTT . . . . .	73
Setting Up a Test Environment . . . . .	75
Writing the MQTT Authentication-Cracking Module in Ncrack . . . . .	77
Testing the Ncrack Module Against MQTT . . . . .	86
Conclusion . . . . .	87

**5****ANALYZING NETWORK PROTOCOLS****89**

Inspecting Network Protocols . . . . .	90
Information Gathering . . . . .	90
Analysis . . . . .	92
Prototyping and Tool Development . . . . .	93
Conducting a Security Assessment . . . . .	93
Developing a Lua Wireshark Dissector for the DICOM Protocol . . . . .	95
Working with Lua . . . . .	95
Understanding the DICOM Protocol . . . . .	95
Generating DICOM Traffic . . . . .	97
Enabling Lua in Wireshark . . . . .	97
Defining the Dissector . . . . .	99
Defining the Main Protocol Dissector Function . . . . .	99
Completing the Dissector . . . . .	100
Building a C-ECHO Requests Dissector . . . . .	101
Extracting the String Values of the Application Entity Titles . . . . .	102
Populating the Dissector Function . . . . .	102
Parsing Variable-Length Fields . . . . .	103
Testing the Dissector . . . . .	104
Writing a DICOM Service Scanner for the Nmap Scripting Engine . . . . .	105
Writing an Nmap Scripting Engine Library for DICOM . . . . .	106
DICOM Codes and Constants . . . . .	106
Writing Socket Creation and Destruction Functions . . . . .	107
Defining Functions for Sending and Receiving DICOM Packets . . . . .	108
Creating DICOM Packet Headers . . . . .	109
Writing the A-ASSOCIATE Requests Message Contexts . . . . .	110
Reading Script Arguments in the Nmap Scripting Engine . . . . .	112
Defining the A-ASSOCIATE Request Structure . . . . .	112
Parsing A-ASSOCIATE Responses . . . . .	113
Writing the Final Script . . . . .	114
Conclusion . . . . .	115

<b>6</b>	<b>EXPLOITING ZERO-CONFIGURATION NETWORKING</b>	<b>117</b>
Exploiting UPnP . . . . .		118
The UPnP Stack . . . . .		119
Common UPnP Vulnerabilities . . . . .		120
Punching Holes Through Firewalls . . . . .		121
Abusing UPnP Through WAN interfaces . . . . .		126
Other UPnP Attacks . . . . .		131
Exploiting mDNS and DNS-SD . . . . .		131
How mDNS Works . . . . .		132
How DNS-SD Works . . . . .		132
Conducting Reconnaissance with mDNS and DNS-SD . . . . .		133
Abusing the mDNS Probing Phase . . . . .		134
mDNS and DNS-SD Man-in-the-Middle Attacks . . . . .		136
Exploiting WS-Discovery . . . . .		145
How WS-Discovery Works . . . . .		145
Faking Cameras on Your Network . . . . .		146
Crafting WS-Discovery Attacks . . . . .		152
Conclusion . . . . .		153

## **PART III: HARDWARE HACKING** **155**

<b>7</b>	<b>UART, JTAG, AND SWD EXPLOITATION</b>	<b>157</b>
UART . . . . .		158
Hardware Tools for Communicating with UART . . . . .		158
Identifying UART Ports . . . . .		159
Identifying the UART Baud Rate . . . . .		162
JTAG and SWD . . . . .		163
JTAG . . . . .		164
How SWD Works . . . . .		165
Hardware Tools for Communicating with JTAG and SWD . . . . .		165
Identifying JTAG Pins . . . . .		166
Hacking a Device Through UART and SWD . . . . .		168
The STM32F103C8T6 (Black Pill) Target Device . . . . .		169
Setting Up the Debugging Environment . . . . .		170
Coding a Target Program in Arduino . . . . .		172
Flashing and Running the Arduino Program . . . . .		174
Debugging the Target . . . . .		181
Conclusion . . . . .		188

<b>8</b>	<b>SPI AND I<sup>2</sup>C</b>	<b>189</b>
Hardware for Communicating with SPI and I <sup>2</sup> C . . . . .		190
SPI 191		
How SPI Works . . . . .		191
Dumping EEPROM Flash Memory Chips with SPI . . . . .		192

I <sup>2</sup> C	197
How I <sup>2</sup> C Works	197
Setting Up a Controller-Peripheral I <sup>2</sup> C Bus Architecture	198
Attacking I <sup>2</sup> C with the Bus Pirate	202
Conclusion	206

## 9 **FIRMWARE HACKING** **207**

Firmware and Operating Systems	208
Obtaining Firmware	208
Hacking a Wi-Fi Modem Router	211
Extracting the Filesystem	212
Statically Analyzing the Filesystem Contents	213
Firmware Emulation	216
Dynamic Analysis	221
Backdooring Firmware	223
Targeting Firmware Update Mechanisms	228
Compilation and Setup	229
The Client Code	229
Running the Update Service	232
Vulnerabilities of Firmware Update Services	233
Conclusion	235

## **PART IV: RADIO HACKING** **237**

### 10 **SHORT RANGE RADIO: ABUSING RFID** **239**

How RFID Works	240
Radio Frequency Bands	240
Passive and Active RFID Technologies	241
The Structure of RFID Tags	242
Low-Frequency RFID Tags	244
High-Frequency RFID Tags	245
Attacking RFID Systems with Proxmark3	245
Setting Up Proxmark3	246
Updating Proxmark3	246
Identifying Low- and High-Frequency Cards	248
Low-Frequency Tag Cloning	249
High-Frequency Tag Cloning	250
Simulating RFID Tags	254
Altering RFID Tags	255
Attacking MIFARE with an Android App	256
RAW Commands for Nonbranded or Noncommercial RFID Tags	258
Eavesdropping on the Tag-to-Reader Communication	260
Extracting a Sector's Key from the Captured Traffic	261
The Legitimate RFID Reader Attack	262
Automating RFID Attacks Using the Proxmark3 Scripting Engine	263
RFID Fuzzing Using Custom Scripting	264
Conclusion	268

<b>11</b>	<b>BLUETOOTH LOW ENERGY</b>	<b>269</b>
How BLE Works . . . . .		270
Generic Access Profile and Generic Attribute Profile . . . . .		271
Working with BLE . . . . .		272
BLE Hardware . . . . .		273
BlueZ . . . . .		273
Configuring BLE Interfaces . . . . .		274
Discovering Devices and Listing Characteristics . . . . .		275
GATTTool . . . . .		275
Bettercap . . . . .		276
Enumerating Characteristics, Services, and Descriptors . . . . .		277
Reading and Writing Characteristics . . . . .		278
BLE Hacking . . . . .		278
Setting Up BLE CTF Infinity . . . . .		279
Getting Started . . . . .		279
Flag 1: Examining Characteristics and Descriptors . . . . .		281
Flag 2: Authentication . . . . .		282
Flag 3: Spoofing Your MAC Address . . . . .		283
Conclusion . . . . .		285
<b>12</b>	<b>MEDIUM RANGE RADIO: HACKING WI-FI</b>	<b>287</b>
How Wi-Fi Works . . . . .		287
Hardware for Wi-Fi Security Assessments . . . . .		288
Wi-Fi Attacks Against Wireless Clients . . . . .		288
Deauthentication and Denial-of-Service Attacks . . . . .		289
Wi-Fi Association Attacks . . . . .		291
Wi-Fi Direct . . . . .		295
Wi-Fi Attacks Against APs . . . . .		299
Cracking WPA/WPA2 . . . . .		299
Cracking into WPA/WPA2 Enterprise to Capture Credentials . . . . .		304
A Testing Methodology . . . . .		305
Conclusion . . . . .		306
<b>13</b>	<b>LONG RANGE RADIO: LPWAN</b>	<b>307</b>
LPWAN, LoRa, and LoRaWAN . . . . .		308
Capturing LoRa Traffic . . . . .		309
Setting Up the Heltec LoRa 32 Development Board . . . . .		309
Setting Up the LoStik . . . . .		314
Turning the CatWAN USB Stick into a LoRa Sniffer . . . . .		318
Decoding the LoRaWAN Protocol . . . . .		323
The LoRaWAN Packet Format . . . . .		323
Joining LoRaWAN Networks . . . . .		324

Attacking LoRaWAN	327
Bit-Flipping Attacks	327
Key Generation and Management	330
Replay Attacks	330
Eavesdropping	331
ACK Spoofing	331
Application-Specific Attacks	331
Conclusion	332

## **PART V: TARGETING THE IOT ECOSYSTEM 333**

### **14**

#### **ATTACKING MOBILE APPLICATIONS 335**

Threats in IoT Mobile Apps	336
Breaking Down the Architecture into Components	336
Identifying Threats	337
Android and iOS Security Controls	339
Data Protection and Encrypted Filesystem	339
Application Sandbox, Secure IPC, and Services	340
Application Signatures	340
User Authentication	340
Isolated Hardware Components and Keys Management	341
Verified and Secure Boot	341
Analyzing iOS Applications	341
Preparing the Testing Environment	342
Extracting and Re-Signing an IPA	343
Static Analysis	344
Dynamic Analysis	347
Injection Attacks	353
Keychain Storage	354
Binary Reversing	355
Intercepting and Examining Network Traffic	356
Avoiding Jailbreak Detection Using Dynamic Patching	357
Avoiding Jailbreak Detection Using Static Patching	358
Analyzing Android Applications	360
Preparing the Test Environment	360
Extracting an APK	361
Static Analysis	361
Binary Reversing	362
Dynamic Analysis	363
Intercepting and Examining Network Traffic	367
Side-Channel Leaks	367
Avoid Root Detection Using Static Patching	368
Avoid Root Detection Using Dynamic Patching	369
Conclusion	370

<b>15</b>	
<b>HACKING THE SMART HOME</b>	<b>371</b>
Gaining Physical Entry to a Building. . . . .	372
Cloning a Keylock System's RFID Tag . . . . .	372
Jamming the Wireless Alarm . . . . .	375
Playing Back an IP Camera Stream . . . . .	379
Understanding Streaming Protocols . . . . .	380
Analyzing IP Camera Network Traffic . . . . .	380
Extracting the Video Stream . . . . .	382
Attacking a Smart Treadmill. . . . .	385
Smart Treadmills and the Android Operating System . . . . .	386
Taking Control of the Android Powered Smart Treadmill. . . . .	387
Conclusion . . . . .	400
 <b>APPENDIX:</b>	
<b>TOOLS FOR IOT HACKING</b>	<b>401</b>
 <b>INDEX</b>	<b>415</b>