Practical Hardware Pentesting

A guide to attacking embedded systems and protecting them against the most common hardware attacks

Jean-Georges Valle

Packt>

BIRMINGHAM—MUMBAI

Practical Hardware Pentesting

Group Product Manager: Wilson D'souza

Publishing Product Manager: Rahul Nair

Senior Editor: Arun Nadar

Content Development Editor: Romy Dias

Technical Editor: Nithik Cheruvakodan

Copy Editor: Safis Editing

Project Coordinator: Neil D'mello

Proofreader: Safis Editing

Indexer: Manju Arasan

Production Designer: Nilesh Mohite

First published: March 2021

Production reference: 1040321

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-78961-913-3

www.packt.com

To my father. I wouldn't be who I am without you.

Contributors

About the author

Jean-Georges Valle is a hardware penetration tester based in Belgium. His background was in software security, with hardware being a hobby, and he then started to look into the security aspects of hardware. He has spent the last decade testing various systems, from industrial logic controllers to city-scale IoT, and from media distribution to power metering. He has learned to attack embedded systems and to leverage them against cloud-scale infrastructure. He is the lead hardware technical expert in an offensive security team of a big four company.

Jean-Georges holds a master's degree in information security and focuses on security at the point of intersection with hardware and software, hardware and software interaction, exploit development in embedded systems, and open source hardware.

I wish to thank my parents for supporting me and loving me unconditionally, Vito and Jon for giving me an opportunity when I needed it, and Ieva for accepting that this book was competing with her for my time and attention.

About the reviewers

Ryan Slaugh has been a maker and breaker of things for over 20 years. Ryan got his start in electrical systems, and augmented his learning to include the analog, digital, embedded, software, and cybersecurity fields. He continues to practice and add to his skill sets in his home lab, and this allows him to do what he loves the most: solve problems with technology. When not working with technology, Ryan enjoys traveling around the globe and exploring the less inhabited areas of the Pacific Northwest. His greatest joy is being with his family on their small hobby farm in Washington State, USA.

Neeraj Thakur is a manager in the risk advisory practice of Deloitte and comes with more than 9 years' experience in the area of information and cybersecurity. He holds a master's degree in cybersecurity from the Indian Institute of Information Technology, Allahabad, and has extensive experience in penetration and security testing of various embedded devices and IoT-enabled products. He is a certified ISA/IEC 62443 cybersecurity fundamentals specialist and has worked extensively in the areas of industrial automation and control system security. He has delivered multiple sessions on IoT and ICS security, as well as in the security community, including Nullcon and CySeck. Neeraj is passionate about reverse engineering and security innovations using Python.

Table of Contents

3
Identifying the Components of Your Target

4
Approaching and Planning the Test

Section 2: Attacking the Hardware

5
Our Main Attack Platform

6
Sniffing and Attacking the Most Common Protocols

7

Extracting and Manipulating Onboard Storage

8

Attacking Wi-Fi, Bluetooth, and BLE

9

Software-Defined Radio Attacks

Section 3: Attacking the Software

10
Accessing the Debug Interfaces

11
Static Reverse Engineering and Analysis

12
Dynamic Reverse Engineering

13
Scoring and Reporting Your Vulnerabilities

14
Wrapping It Up – Mitigations and Good Practices