HACK THE SIGNAL

HACK THE SIGNAL

A curious hacker's guide to hardware & protocol reverse engineering

NIEL NIELSEN

SEC1.DK

HACK THE SIGNAL

A curious hacker's guide to hardware & protocol reverse engineering

NIEL NIELSEN
SEC1.DK

Contents

Chapter 1

Preface: Before You Touch Anything

This book began as a blog. Posts about pulling firmware from a sealed device, building an RFID reader out of a handful of nRF52840 peripheral registers, disassembling a bootloader to answer a question that nagged at me for weeks. Each post was complete on its own: a problem, the false starts, the fix, what the fix taught me.

What you are holding is those posts reorganised into something with a spine. The problem they collectively answer is: *how do you get started in hardware reverse engineering when nobody hands you a syllabus?*

1.1 Who this is for

You are curious. You can write a small script, read a block of C without panicking, and you have probably taken apart something you should not have. You do not necessarily have a formal background in electronics or security. You have heard the words “RFID attack” or “firmware dump” and wanted to know what they actually mean in practice, from someone who has done them rather than described them abstractly.

This book is not for people who already know this field. It is for people on the outside of the field, looking for a door.

1.2 The hardware thread

Every hands-on section in this book uses one device: the **ChameleonUltra**. It is an open-source, open-hardware RFID research tool built on the Nordic nRF52840, an ARM Cortex-M4 with an integrated 2.4 GHz radio and a dedicated NFC peripheral. It does LF and HF RFID. It reads, emulates, and sniffs. It connects over USB-C and BLE. It costs around $60 from the usual channels and the full schematic is on GitHub.

The reason I chose one device rather than a toolkit is that depth beats breadth for learning. By the end of this book you will understand one piece of hardware well enough to modify its firmware, debug its peripherals, and extend its protocol support. That skill transfers. The ChameleonUltra is the vehicle, not the destination.

You will need:

- One ChameleonUltra (RfidResearchGroup edition or NielDK fork, both work)
- A USB-C cable
- A Linux machine or VM (the examples use Arch Linux, but any distro works)

- A handful of RFID cards to practise on: a hotel key, a transit card, a parking fob

For Chapters 11 and 12 you will not use the ChameleonUltra at all. Those chapters cover embedded Linux targets and endpoint security. Different territory, same methodology.

1.3 How wrong turns work here

Every chapter in this book includes the dead ends. The hypothesis that looked solid until one byte contradicted it. The firmware bug that crashed the device in a way that pointed nowhere obvious. The five wrong theories about a bootloader, killed in order.

This is deliberate. In real reverse engineering work, the dead ends are where the learning happens. A tidy account that skips from question to answer teaches you the answer. A messy account that shows you *how to eliminate wrong answers* teaches you to think.

When you see a section labelled “Dead End” or a hypothesis killed by evidence, read it carefully. That is the part most textbooks leave out.

1.4 Building this book yourself

The source for this book is Pandoc-flavoured Markdown. To build an epub or PDF from source:

```
# Install Pandoc (Arch Linux)
sudo pacman -S pandoc

# Build epub
pandoc --metadata-file=metadata.yaml --toc --number-sections \
  -o hack-the-signal.epub ch00-preface.md ch01-*.md ... ch13-*.md

# Build PDF (requires texlive)
pandoc --metadata-file=metadata.yaml --pdf-engine=xelatex \
  -o hack-the-signal.pdf ch00-preface.md ch01-*.md ... ch13-*.md

# Or use the build script
chmod +x build.sh && ./build.sh
```

The source lives at `sec1.dk` alongside the original blog posts it grew from.

1.5 A note on cost

This book is free. If it saves you hours of dead ends or points you at something you would not have found otherwise, a small donation is appreciated but never expected: paypal.me/nieldk

---

Let’s start with what is actually inside the devices you want to hack.

Redigering: Niel Nielsen
Korrektur: Niel Nielsen
Bidragsydere: Niel Nielsen

Forlag: BoD · Books on Demand, Strandvejen 100, 2900 Hellerup, bod@bod.dk
Tryk: Libri Plureos GmbH, Friedensallee 273, 22763 Hamburg

ISBN: 978-87-430-9123-3