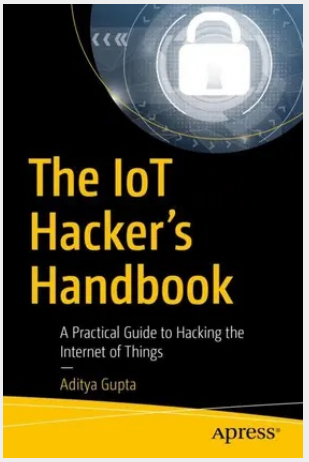
Gupta

# The IoT Hacker's Handbook

A Practical Guide to Hacking the Internet of Things




**58,84 €**
54,99 € (zzgl. MwSt.)

*sofort versandfertig, Lieferfrist: 1-3 Werktage*

Take a practioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture.
You'll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware.

As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. *The IoT Hacker's Handbook* breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely.
**What You'll Learn**

- Perform a threat model of a real-world IoT device and locate all possible attacker entry points
- Use reverse engineering of firmware binaries to identify security issues
- Analyze,assess, and identify security issues in exploited ARM and MIPS based binaries
- Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee

**Who This Book is For** Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Take a practioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture.
You'll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware.

As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely.
What You'll Learn- Perform a threat model of a real-world IoT device and locate all possible attacker entry points
- Use reverse engineering of firmware binaries to identify security issues
- Analyze,assess, and identify security issues in exploited ARM and MIPS based binaries- Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee

Who This Book is For
Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

**Artikelnummer:** 9781484242995
**Medium:** Buch
**ISBN:** 978-1-4842-4299-5
**Verlag:** Springer Nature B.V.
**Erscheinungstermin:** 01.04.2019
**Sprache(n):** Englisch
**Auflage:** 1. Auflage 2019
**Produktform:** Kartoniert
**Gewicht:** 516 g
**Seiten:** 320
**Format (B x H):** 156 x 233 mm



**Kundenservice Verlag Dr. Otto Schmidt KG**
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)