



Joe Grand's Hands-off Hardware Hacking Training Course Agenda

Last updated: July 20, 2026

This two-day comprehensive course teaches fundamental hardware hacking techniques and processes used to reverse engineer and defeat the security of electronic devices. It combines material from Joe Grand's [hardware hacking training courses](#) and his most popular [hardware security research](#), while removing the hands-on elements in order to provide access to a wider audience. This course can be held in-person or online.

A. Overview

1. Hardware hacking objectives and motivations
2. Common attack vectors
3. Methodology and process

B. Information Gathering

1. Open-source intelligence
2. Patents and certifications
3. Obtaining and reading data sheets

C. Product Teardown

1. Opening housings
2. Anti-tamper mechanisms
3. Coatings and encapsulation
4. Component identification

D. Printed Circuit Boards (PCBs)

1. PCB construction and fabrication
2. Board-level reverse engineering and modification
3. Soldering and desoldering

E. Buses and Interfaces

1. Identifying interfaces
2. Determining pin function
3. Signal monitoring and analysis
4. Signal manipulation and spoofing
5. Debug interfaces

F. Memory and Firmware

1. Firmware extraction
2. Firmware analysis and modification
3. Microcontroller code protection
4. Secure boot and trusted execution environments

G. Advanced Techniques

1. Fault injection
2. Side channel attacks
3. Chip-level reverse engineering and manipulation

H. Hardware Espionage

1. Supply chain risks and threats
2. Hardware implants
3. Covert channels and data exfiltration