Joe Grand's Hardware Hacking Advanced Training Course Agenda (NFI)

Last updated: May 17, 2022

Prerequisite: Joe Grand's Hardware Hacking Basics two-day training

This two-day course focuses on advanced hardware hacking tools and techniques commonly used by digital forensic investigators. It is a hands-on environment where students will access and exploit various real-world products. Each section contains an overview, examples, and hands-on exercises.

A. Hardware Implants and Espionage

- Build a keystroke-injection hardware implant, experiment w/ various payloads

B. JTAG Discovery

- Locate debug interface of an off-the-shelf embedded system w/ JTAGulator

C. Firmware Extraction

- Extract memory contents via JTAG
- Extract memory contents via UART/bootloader
- Extract memory contents via physical access w/ device programmer

D. Side Channel Attacks

- Defeat PIN protection of custom circuit board via timing measurements

E. Fault Injection

- Extract program code from a protected microcontroller via voltage glitch w/ ChipWhisperer

F. Forensic Challenges

Apply the knowledge and skills learned in the course to attack real-world embedded systems. Examples include extracting data from a WiFi router, IoT camera, car infotainment system, and/or password-protected hard drive. Exercises subject to change based on device availability.

G. Open Lab/Case-Specific Projects