# Hardware Hacking Bootcamp: Syllabus

## VoidStar Security LLC

### Description

This five-day course is designed to teach the fundamentals of hardware reverse engineering and analysis. With a focus on understanding the low-level protocols that comprise embedded systems, students learn how interfaces such as SPI, I2C, JTAG, SWD work while developing tools to interface with these protocols.

### Course Objectives

After participating in this course, students will have experience with:

- Non-Invasive hardware analysis (component identification, etc.)
- Tracing and identifying points of interest on PCBs
- Extracting firmware over multiple interfaces
- Unpacking / analyzing binary blobs
- Attacking hardware debuggers (JTAG, ETC)
- Modifying, repacking, and reflashing firmware

Students will learn how to augment existing tools to work around problems when extracting firmware.

Labs include extracting SPI/I2C based flash chips, discovering and gaining access to consoles using UART, and identifying, enumerating, and actuating hardware-level debuggers such as JTAG and SWD.

All exercises and laboratories are performed using open source tooling on a Raspberry Pi. The Raspberry Pi will be used to attack and exploit all of the targets included in the kit. The tools and techniques used throughout the course were chosen specifically due to their portability across various hardware platforms.

Upon completion of the course, students will receive:

- A certificate of completion
- All slides for the course materials
- Video recorded lectures from the course (if remote)
- An SD card containing the software and tooling used for the Raspberry Pi

### Course Structure

This course includes multiple modules, one for each protocol of interest. For each module, we will perform the following:

- Protocol Overview and Analysis
- Understanding and Reviewing Captured Protocol Traffic
- Protocol Analysis from a Reverse Engineering Perspective
- Tools for Reverse Engineering Specific Protocols
- Practical Attacks and Applications on Provided Targets

After each protocol module, a target analysis will be performed to reinforce what was learned in the analysis segment. Using this knowledge, students will perform hardware attacks on the targets included in their kits.

The targets include a travel router, Transcend SSD, a modern ARM-based USB controller, and an arcade cabinet where students will hack it to achieve a high score. Students will extract firmware, analyze the resulting data, and perform hardware attacks on each target.

## Requirements

This course is targeted towards security researchers who want to learn more about the process of firmware extraction and embedded systems analysis. Students should be familiar with the Linux command line and be comfortable with a scripting language such as python. C experience is also helpful but not required.

Interfacing with the Raspberry Pi requires an available USB type A port. A virtual machine is provided to automate the configuration of the Raspberry Pi. Students should be able to load and run virtual machines if they are not comfortable installing Pulseview and configuring an ethernet interface on their host machine.

## Pricing and Private Offerings

Public and private versions of this course are available. The class size for remote courses is limited due to exercise complexity.

For private remote offerings, alternate timings can be arranged; for example, a course can be performed over the course of multiple weeks once a week, etc.

| Course Type | Location | Minimum Number of Students | Cost Per Student |
|---|---|---|---|
| Public | Remote | 5 | $2500 |
| Private | Remote | 5-8 | $2750 |
| Private | Onsite | 5 | $3000 + Travel fees |
| Private | Onsite | 5+ (max of 20) | $2750 + Travel fees |

If you are interested in taking this course, or organizing a private offering, please reach out to contact@voidstarsec.com