Hands-On Hardware Hacking: Advanced Training Course Agenda

Last updated: October 14, 2016

This one-day class focuses on system manipulation and memory extraction via on-chip debug interfaces. It is a hands-on, informal environment where students are able to experiment with a variety of electronic products and hardware hacking tools and techniques.

Students should have completed Grand Idea Studio's Hands-On Hardware Hacking and Reverse Engineering training course (www.grandideastudio.com/portfolio/hardware-hacking-training/) or have prior hardware hacking knowledge and experience.

A. Side Channel Timing Attack

1. Discover side channel weakness on a custom circuit board
2. Defeat power-on PIN protection via timing measurements

B. Firmware Extraction/Modification

1. Locate programming/debug interface on a custom circuit board
2. Extract firmware using vendor-specific tools
3. Determine security mechanism via disassembly and debugging
4. Modify and inject new firmware to bypass security

C. JTAG Deep Dive

1. Interface specifications/functionality
2. Tool setup/usage (including JTAGulator, OpenOCD, UrJTAG, gdb)
3. Demonstrations and open lab
    - Locate JTAG connections on target hardware via manual or automated methods
    - Retrieve chip information
    - Explore target hardware via JTAG (debugging, memory modification, firmware extraction)
    - Examine file system and/or determine security mechanism (if any)