Firmware Extraction and Advanced Manipulation Workshop Agenda

Last updated: November 22, 2018

This one-day workshop focuses on system manipulation and memory extraction via on-chip debug interfaces. It is a hands-on environment where students will exploit bare metal and Linux-based embedded systems using advanced techniques.

Prerequisite: Joe Grand's Hardware Hacking Basics two-day training (www.grandideastudio.com/portfolio/hardware-hacking-training/)

A. Side Channel Timing Attack

1. Overview and examples
2. Discover side channel weakness on a custom circuit board
3. 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 Exploitation

1. Interface specifications/functionality
2. Tool setup/usage (including OpenOCD, gdb, UrJTAG, and JTAGulator)
3. Gain root access on a Linux-based embedded system through memory modification