Joe Grand's Firmware Extraction and Advanced Manipulation Workshop Agenda

Last updated: May 22, 2020

This one-day workshop focuses on firmware extraction and system manipulation via on-chip debug interfaces. It is a hands-on environment where students will exploit bare metal and Linux-based devices using a variety of techniques.

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

A. Firmware Modification

1. Overview of vendor-specific debug interfaces
2. Locate debug interface of custom circuit board w/ manual techniques
3. Extract firmware via vendor-specific tools
4. Determine security mechanism via disassembly
5. Modify and inject new firmware to bypass security

B. JTAG Detection

1. Overview of JTAG specification/functionality
2. Locate debug interface of off-the-shelf embedded system w/ JTAGulator
3. Extract firmware via JTAG
4. Extract firmware via physical memory access w/ device programmer
5. Explore/analyze firmware contents

C. JTAG Exploitation

Apply the skills learned in the workshop to gain root access on a Linux-based single board computer through multiple methods of real-time kernel patching.