Joe Grand's Firmware Extraction and Manipulation Workshop Agenda

Last updated: February 21, 2024

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

A. JTAG Discovery

1. Overview of debug interfaces, JTAG specification/functionality
2. Locate debug interface of off-the-shelf embedded system w/ JTAGulator

B. Firmware Extraction

1. Extract firmware via JTAG
2. Extract firmware via UART/bootloader
3. Extract firmware via physical memory w/ device programmer
4. Explore/analyze firmware contents

C. Firmware Modification

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

D. Privilege Escalation

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