Joe Grand's Defeating Microcontroller Code Protection Workshop Agenda

DRAFT: SUBJECT TO CHANGE

Last updated: May 25, 2020

This one-day workshop teaches advanced techniques used to defeat the security features of microcontrollers meant to protect against unauthorized memory access. It is a hands-on environment where students will use a variety of hardware tools and real-world targets. Each section provides details of the microcontroller's code protection features and its corresponding attack methodology.

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

A. Microcontroller Security Overview

B. STMicroelectronics STM32

- Hands-on exercise: Locate debug interface, extract program code from a protected STM32F103 microcontroller via debug interface, identify differences between original and extracted code

C. ARM Cortex-M0

- Hands-on exercise: Extract program code from a protected nRF51822 microcontroller via debug interface, reload code into device with code protection disabled, debug code to verify proper functionality

D. Microchip PIC

- Hands-on exercise: Extract program code from a protected PIC18F4520 via multi-stage attack, disassemble and analyze extracted code

E. Other Techniques

- Discussion of additional attack techniques, including optical, timing, and glitching/fault injection