GRAND IDEA STUDIO

Joe Grand's Defeating Microcontroller Code Protection Workshop Agenda

Last updated: February 21, 2024

This one-day workshop teaches advanced techniques used to defeat the security features of microcontrollers meant to protect against unauthorized 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

A. Microcontroller Security Overview

B. Fault Injection

- Hands-on exercise: Extract program code from a protected NXP LPC1114 via voltage glitch using the ChipWhisperer

C. Register Manipulation

- Hands-on exercise: Extract program code from a protected Nordic Semiconductor nRF51822 microcontroller via register and program flow manipulation

D. Interrupt Vector Manipulation

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

E. Side Channel Timing Attack

- Hands-on exercise: Discover side channel weakness on a custom circuit board, defeat PIN protection via timing attack

F. Other Techniques