Firmware Analysis Fundamentals: Syllabus and Overview

VoidStar Security LLC

2023-11-01

Firmware Analysis Fundamentals: Syllabus and Overview

VoidStar Security LLC

Course Description

- Course Length: 24 Hours
- Course Availability: Onsite, Remote, Self-Paced

This course aims to equip attendees with the skills to analyze and assess embedded firmware for vulnerability assessment and forensics purposes. Students will solve challenges running on real hardware using the provided target (the PWNtroller). Students will learn how to load bare metal firmware images into Ghidra and create their own loader plugins and scripts to solve the provided challenges. The challenges will focus on analyzing specific peripherals and protocol usage by the PWNtroller firmware and require students to answer questions, write scripts, and solve puzzles to move on to the next challenge.

Course Objectives

After participating in the course, students will have experience in the following:

- Loading and analyzing bare-metal firmware images into Ghidra
- Reviewing and understanding CPU datasheets for reverse engineering
- Extending Ghidra for firmware analysis via Python and Java-based plugins
- Developing custom loaders for firmware images
- Emulating segments of firmware images using PCode
- Utilizing Ghidra's debugger for both bare metal and emulated targets

Upon completion of the course, students will receive:

- A certificate of completion
- All slides for the course materials
- A virtual machine including all tools and exercises
- Video recorded lectures from the course (if remote)
- Access to a Discord channel with past students of VSS courses

Course Outline

- Module 1: Ghidra Usage and Navigation

  - Installing / Building Ghidra
  - Feature Overview
  - Basic navigation

- Module 2: PWNtroller Target Review
  - Device features
  - **Lab:** Connecting to the PWNtroller
- Module 3: ARM Architecture Review
  - ARM/Thumb/Aarch64 Review
  - Understanding and Labelling Interrupt vectors
  - ARM exception levels and exception handling
  - Memory-mapped peripherals
- Module 4: Firmware Analysis - First Steps
  - Determining the format(s) of a firmware image
  - Working with compressed/encrypted firmware
  - Extracting components of interest from a firmware image
- Module 5: Loading Firmware Into Ghidra
  - **Lab:** Determining the load address
  - **Lab:** Locate the entry point for the firmware image
  - **Lab(s):** How to create a memory map
- Module 6: Peripheral Creation in Ghidra
  - Overview of embedded peripherals
  - Creating memory maps in Ghidra
  - **Lab:** Creating peripheral models in Ghidra
- Module 7: Extending Ghidra
  - **Lab:** Eclipse setup and integration for plugin development
  - **Lab:** Label IO Peripherals with Ghidra's Python API
  - **Lab:** Create a memory map with Ghidra's Java API
  - **Lab:** Develop a loader for the PWNtroller
- Module 8: Augmenting and Improving Ghidra's Default Analysis
  - **Lab:** Dealing with ARM/Thumb code
  - **Lab:** Improving decompiler output
  - **Lab:** Improving decompiler output

  - **Lab:** Creating structures and enums

- Module 9: Debugging Binaries with Ghidra
  - Debugger usage and overview
  - **Lab:** Connecting Ghidra's debugger to Qemu
  - **Lab:** Introduction to OpenOCD
  - **Lab:** Connecting Ghidra's debugger to physical hardware via OpenOCD
  - **Lab:** Emulating Firmware with PCode
- Final Module: PWNtroller Exercises:
  - Challenge Zero: Programming the PWNtroller
  - Challenge One: Unlocking the UART
  - Challange Two: Secrets in SRAM
  - Challange Three: SPI-ing on Firmware
  - Challenge Four: I see the I2C
  - Challange Five: GPIO
  - Challenge Six: Dastardly Decompression
  - Challenge Seven: Mass Storage Mischief
  - Challenge Eight: Instruction Tracing
  - Final Challenge: Disarming the PWNtroller

Target Audience / Pre-requisites

This course aims at security researchers and engineers who want to learn more about firmware analysis and security. Students should be familiar with the Linux command line and comfortable with a scripting language like Python. C experience is also helpful but not required. While some hardware experience will be beneficial, it is optional for this course.

Before taking this course, it is recommended that students review the VoidStar Security introductory Ghidra course provided **here.**

Pricing

Public and private versions of this course are available. The class size for remote courses is limited due to exercise complexity. For some courses, self-paced online variants are provided. These versions cover the core concepts but do not include bonus exercises and additional background information that arises from classroom discussion.

Course Type	Location	Minimum Number of Students	Cost Per Student (USD)
Private	Onsite	10	$1500
Private	Onsite	5	$2000

If you are interested in taking this course or organizing a private offering, please reach out to contact@voidstarsec.com