VSS 301: Firmware Analysis Fundamentals

Description

This course is designed to provide students with an understanding of firmware reverse engineering techniques and tools, with a focus on the use of Ghidra. This course is designed to provide students with a comprehensive understanding of software reverse engineering using the powerful reverse engineering tool Ghidra. Ghidra is a free and open-source software reverse engineering (SRE) framework developed by the National Security Agency (NSA).

VSS 301 will cover the use of Ghidra for reverse engineering firmware binaries for different architectures, including ARM and MIPS. Students will learn Ghidra scripting, processor module development, extension development, and emulation techniques using Ghidra's PCode. The course will be largely focused on laboratory exercises designed to teach students how to get started when performing black box analysis of a firmware binary.

Throughout the course, students will learn how to use Ghidra to reverse engineer various types of software, including executables, libraries, and firmware. The course will cover the basics of Ghidra's user interface and features, including the Code Browser, Decompiler, and Assembler, and how to use them effectively. Students will also learn how to use Ghidra's powerful scripting and automation capabilities to aid in reverse engineering tasks.

Objectives

- Understand the principles of firmware reverse engineering and the importance of understanding firmware in embedded systems
- Learn how to use Ghidra for reverse engineering firmware binaries for different architectures
- Review ARM and MIPS architectures and their assembly languages
- Develop the ability to analyze and interpret firmware binary code
- Gain practical experience in the use of firmware reverse engineering techniques through hands-on lab exercises
- Learn how to write Ghidra script to automate task, Create processor modules and Ghidra extensions

Outline

- Introduction to Firmware Reverse Engineering
    - Overview of firmware reverse engineering and its role in embedded systems
    - Importance of understanding firmware in embedded systems
    - Overview of firmware reverse engineering tools and techniques
- Ghidra Introduction
    - Overview of Ghidra
    - Installation and setup of Ghidra
    - Understanding Ghidra's interface and its features
- Reverse Engineering Techniques
    - Overview of reverse engineering techniques for different architectures including ARM and MIPS
    - Hands-on lab exercises to practice reverse engineering firmware binaries for different architectures
- Ghidra Scripting
    - Introduction to Ghidra script and its components
    - Hands-on lab exercises to practice writing Ghidra script to automate tasks
- Processor module and Extension Development
    - Overview of Ghidra's processor module development process
    - Hands-on lab exercises to practice creating processor module and extension
- Emulation and PCode
    - Overview of emulation techniques using Ghidra's PCode
    - Hands-on lab exercises to practice firmware emulation
- Conclusion
    - Summary of key concepts and techniques covered in the course
    - Discussion of the future of firmware reverse engineering and its potential impact on embedded systems

Outcomes

Throughout the course, students will work on hands-on lab exercises and real-world projects that will give them the opportunity to apply the concepts and techniques learned in the course to real-world scenarios. Upon completion of the course, students will have a deep understanding of software reverse engineering and the ability to effectively use Ghidra to reverse engineer software, identify vulnerabilities, and automate reverse engineering tasks.

Prerequisites

The course is designed for students with some experience in programming, as well as a basic understanding of computer architecture and assembly language. Familiarity with a Linux environment is also recommended.

Schedule / Pricing

Duration: 4 Days
Cost Per Student: $3,000