DRIEI
PhD Program in Electronic and Computer Engineering
University of Cagliari, Italy

Course:	Reverse Engineering and Low-Level Program Analysis
Instructor:	Davide Maiorca
SSD:	ING-INF/05
Credits / hours:	3 credits / 24 hours
Language:	English
Scheduling:	September 2024
Final Exam:	Project
Website:	N/A

Goal of the Course

Reverse Engineering (RE) is a discipline that can be employed to analyze the functionality of programs without having the related source code. Thanks to RE, it is possible to understand the bugs of a program, extract its possible hidden functionalities, and change its whole behavior. This course will provide the essential tools to understand and analyze the low-level behavior of a program. In the first week, we provide an overview of programs written in Assembly X86/64 and static and dynamic techniques for their analysis. In the second and third weeks, the focus will be shifted to programs written in MIPS and ARM. The course will employ a game-based approach, where students will consolidate the topics through challenges taken from the world of capture-the-flag (CTF).

Prerequisites

None, but the seminar is especially recommended for students who have already completed the course "Web Security and Malware Analysis."

Intersection with other courses at the University of Cagliari

The first part of the course will review some topics that are explained in the “Web Security and Malware Analysis” course.

Course Outline

Week 1 - X86-64 Reverse Engineering (8 hours):

- Structure of ELF files

- Process Structure in Memory

- Registers and Opcodes

- Conditional and control instructions

- Execution of functions and subroutine calls
- Disassembling and Decompilation tools
- Dynamic Analysis fundamentals
- Practice exercises

Week 2 - MIPS Reverse Engineering (8 hours):

- Introduction to the MIPS architecture
- MIPS cross-compiling and execution
- Opcodes and registers
- Loading and storing
- Control instructions, branching, and setting
- Calling functions - the structure of the stack
- Practice exercises

Week 3 - ARM Reverse Engineering (8 hours):

- Introduction to the ARM architecture
- ARM cross-compiling and execution
- ARM vs. X86 registers
- ARM instructions and Thumb mode
- Loading and storing
- Branches
- Function calls and stack
- Practice exercises