



UNICA  
UNIVERSITÀ  
DEGLI STUDI  
DI CAGLIARI



sAifer Lab  
Joint lab on Safety and Security of AI

## Reverse Engineering and Low-Level Program Analysis Faculty of Engineering and Architecture Ph.D. Program in Electronic Engineering and Computer Science

**Lecturer:** Prof. Davide Maiorca - [davide.maiorca\[at\]unica\[dot\]it](mailto:davide.maiorca@unica.it)

**Language:** English

**Target students:**

Ph.D. Students (DRIEI)

National Ph.D. Students

Master's Degree Students in Computer Engineering, CyberSecurity, and Artificial Intelligence

Master's Degree Students in Internet Engineering

Master's Degree Students in Electronic Engineering

### 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).

### Requirements

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

**Topics:**

- 8 hours – Assembly X86/64 Basics - Static and Dynamic Analysis - Practice Exercises
- 8 hours - Fundamentals of MIPS reversing - Practice Exercises
- 8 hours – Fundamentals of ARM reversing - Practice Exercises

**Detailed Table of Contents:**

Week 1 (Feb 10th and 14th) - X86-64 Reverse Engineering:

- 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 (Feb 17th and 20th) - MIPS Reverse Engineering:

- 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 (Feb 24th and 28th) - ARM Reverse Engineering:

- 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

**Credits:** 3 for Ph.D. Students and 2 for Master's Degree Students. The credits will be given after having passed a final test.

**Registrations for the seminar are open, and the course will start on February 10th, 2025. Lectures will be provided in person and NO streaming will be provided. To register, please fill this form by February 9th, 2025:**

<https://forms.office.com/e/Q1fvFajUbc>

**Important Dates and Seminar Schedule (2025):**

The seminar will be held on February 10<sup>th</sup>, 14<sup>th</sup>, 17<sup>th</sup>, 20<sup>th</sup>, 24<sup>th</sup> and 28<sup>th</sup>. Time: 9:30 to 13:30 (4 hours lecture/day)

Location: Room BA for all lectures except for the 14<sup>th</sup> and the 20<sup>th</sup> (Room AB)