CS 577-A Reverse Engineering & Application Analysis

Department of Computer Science, School of Engineering

Fall 2021

COURSE DESCRIPTION

Introduction to reverse engineering of binary code and its applications in the context of computer security. Students will be introduced to knowledge about binary code and how it interacts with the operating system, skills for statically disassembling binary code and dynamically tracing the execution of binary code, and capabilities of understanding the behaviors of binary code based on static disassembly or dynamic tracing. Students will be introduced to tools for parsing, disassembling, decompiling, tracing, and debugging binary code. Students will also be introduced to the application of reverse engineering of binary code in vulnerability finding and malware analysis.

STUDENT LEARNING OUTCOMES

After successful completion of this course, students will be able to:

- Understand the format, structure, and contents of binary code
- Understand how binary code interacts with the operating system
- Parse, disassemble, and decompile binary code with static analysis tools
- Run, debug, and trace binary code with dynamic analysis tools
- Understand the behaviors of binary code based on static analysis and dynamic analysis
- Reverse engineering binary code to capture hidden vulnerabilities
- Reverse engineer IoT samples to understand their contents, functionality, and security issues

COURSE MATERIALS

Textbook

- Reverse Engineering for Beginners (available at https://beginners.re (Links to an external site.) for free)

Suggested Readings (if you want to learn deeper and broader):

- https://github.com/wtsxDev/reverse-engineering#books (Links to an external site.)

Course Platform:

- REMnux (default option):

  https://docs.remnux.org (Links to an external site.)
  - Please run it as a Virtual Machine (you can run it with VirtualBox, the free VM hypervisor)
  - Please build the VM from scratch with a minimal Ubuntu (https://docs.remnux.org/install-distro/install-from-scratch (Links to an external site.)). Otherwise, the VM will be extremely slow

Tools:

- Disassembler and Decompiler:

  https://www.nsa.gov/resources/everyone/ghidra (Links to an external site.)
  - Please run it inside the VM
- BinWalk: https://github.com/ReFirmLabs/binwalk (Links to an external site.)

FORMAT AND STRUCTURE

This course is comprised of one lecture per week, in-class practices, homework assignments, and a course project.