CMPSC 595G: Topics in Binary Analysis

Colin Unger

January 10, 2020

Instructor: Colin Unger
Email: colinunger@ucsb.edu
Shellphish Slack: @lockshaw
Office Hours: On demand
Lecture: Friday 4:30–6:30pm, HFH 1132
Course Website: cs595g.lockshaw.io/w20.html
Description:
A reverse engineer today relies on a multitude of tools: a dissasembler, a symbolic execution engine, a decompiler, an assembler, a debugger, etc. The list goes on and on. This class will go over both how these tools and how to build them. You will implement at least the basics of an emulator, a loader, a disassembler, a symbolic execution engine, and a decompiler and use them in reverse engineering tasks. In addition, we will cover the basics of program analysis foundations (dataflow analysis).
Assignments & Grading:
The class will be split into groups of 3. The only assignments in the course will be a series of CTF-style challenges. Most weeks, a new set of challenges will be posted, some required and some optional. To pass the class, all required challenges must be solved.
Outline:
Note that this outline is preliminary and will almost certainly change throughout the quarter.

- Week 1: January 10

  Topics:

  - Class Introduction
  - Introduction to CTFs
  - Logistics, Assignments, and Grading
  - Ghidra, Decomperson

- Week 2: January 17

  Topics:

  - x595g Architecture
  - Executable File Formats (ELF, YFF)

  - Linkers
  - Loaders

- Week 3: January 24
  Topics:
  - Disassemblers
- Week 4: January 31
  Topics:
  - Symbolic Execution
- Week 5: February 7
  Topics:
  - Symbolic Execution Week 2
- Week 6: February 14
  Topics:
  - Dataflow Analysis
- Week 7: February 21
  - Decompilers Week 1
- Week 8: February 28
  - Decompilers Week 2
- Week 9: March 6
  No class! (UCSB iCTF)
- Week 10: March 13
  - Decompilers Week 3
- Finals Week:
  No class! Good look on your finals!