# CSE 410/510 Special Topics: Software Security

Dates: 8/29/2022 - 12/5/2022
Time: Monday 5:00 PM - 7:50 PM

Instructor: Dr. Ziming Zhao
Email: zimingzh@buffalo.edu
Office Hours: Monday 3:30 PM - 4:30 PM or by appointment
You will need to log in to UB Zoom before you join the office hours at
`https://buffalo.zoom.us/j/95299258797?pwd=QlBhbjJIUlM5WmlETmFtOE5qT1Z5dz09`

TA: Md. Armanuzzaman Tomal
Email: mdarmanu@buffalo.edu
Office Hours: Friday 3:30 PM - 4:30 PM or by appointment
You will need to log in to UB Zoom before you join the office hours at
`https://buffalo.zoom.us/j/95299258797?pwd=QlBhbjJIUlM5WmlETmFtOE5qT1Z5dz09`

## 1 Course Description

This course is designed to provide students with good understanding of the theories, principles, techniques and tools used for software and system hacking and hardening. Students will study, in-depth, binary reverse engineering, vulnerability classes, vulnerability analysis, exploit and shellcode development, defensive solutions, etc. to understand how to crack and protect native software. In particular, this class covers offensive techniques including stack-based buffer overflow, heap security, format string vulnerability, return-oriented programming, etc. This class also covers defensive techniques including canary, shadow stack, address space layout randomization, control-flow integrity, etc. A key part of studying security is putting skills to the test in practice. Hacking challenges known as Capture The Flag (CTF) competitions are a great way to do this. In this class the progress of students are evaluated by lab assignment and in-class Capture-The-Flag (CTF) competitions.

## 2 Student Learning Outcomes

1. Identify the aforementioned types of software vulnerabilities at source code and binary code level

2. Exploit the discovered software vulnerabilities

3. Understand the existing defensive mechanisms to defeat attacks, their pros and cons

## 3 Topics

1. Background knowledge

    (a) Principles of compiler, linker and loader

    (b) x86 and x86-64 architectures

    (c) x86 and x86-64 instruction sets

    (d) Assembly and reversing engineering with AT&T and Intel syntax

    (e) Linux file permissions

    (f) Set-UID programs

    (g) ELF file format, PLT, GOT

    (h) Memory map of a Linux process (x86 and x86-64)

(c) Jump-oriented programming

(d) Control-flow integrity (CFI)

(e) Tools: `ROPgadget, pwntools`

9. Data-oriented attacks

(a) Direct data manipulation

(b) Data-oriented programming

10. Race conditions

(a) Race in file system

(b) Process and thread

(c) Race in memory

# 4  Grading Policy

Students will be evaluated on their performance on the homework, exams and CTFs. Attendance check will be performed in each class. Table 4 shows the grade breakdown.

| Area | No. Items | Points per Item | Points for Area |
|------|-----------|-----------------|-----------------|
| Homework | 14 | 45 | 630 |
| CTFs | 2 | | 360 |
|     Midterm CTF | 1 | 160 | |
|     Final CTF | 1 | 200 | |
| Attendance | 14 | 1 | 14 |
| Anonymous Course Evaluation Bonus | 2 | 10 | 20 |
| Total | | | 1024 |

Table 1: Grades Breakdown

| Points | Grade |
|--------|-------|
| 930 - | A |
| 900 - 930 | A- |
| 870 - 900 | B+ |
| 830 - 870 | B |
| 800 - 830 | B- |
| 770 - 800 | C+ |
| 700 - 770 | C |
| 670 - 700 | D+ |
| 600 - 670 | D |
| 0 - 600 | F |

Table 2: Final Letter Grades

# 5  Prerequisite

Students are expected to have a background in the C programming language (CSE 220 Systems Programming or equivalent). Solid background from the following classes helps significantly: i) CSE 341 Computer Organization; ii) CSE 365 Introduction to Computer Security; iii) CSE 421/521 Operating Systems. The instructor strives to keep this class self-contained.

# 6 Plagiarism and Cheating

Students are encouraged to discuss the assignments online and offline. However, students are not allowed to share code, exploits, write-ups with other students.

Plagiarism or any form of cheating in homework, assignments, labs or exams is subject to serious academic penalty. As an institution of higher learning, UB expects students to behave honestly and ethically at all times, especially when submitting work for evaluation in conjunction with any course or degree requirement. All students are encouraged to become familiar with UB's Academic Integrity Policy (`https://www.buffalo.edu/academic-integrity.html`), Honor Code, and Student Conduct Policy. There is a zero tolerance policy in this class. Any violation of the academic integrity policy will result in a `0` on the homework, lab or assignment, and even an `F` or `>F<` on the final grade. The violation will be reported to the department chair and the Dean's office. The instructor takes plagiarism very seriously, e.g., in Spring 2018, two students received an `F` for plagiarism behaviors.

# 7 Syllabus Update

Information in the syllabus may be subject to change with reasonable advance notice.