CSE 610 Special Topics: System Security - Attack and Defense for Binaries

Dates: 08/31/2020 - 12/11/2020
Location: Online
Time: Monday, 5:20 PM - 8:10 PM

Instructor: Dr. Ziming Zhao
Email: zimingzh@buffalo.edu
Office: 338B Davis Hall
Office Hours: By Appointment

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/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-based buffer overflow, format string vulnerability, return-oriented programming, etc. This class also covers defensive techniques including canary, shadow stack, address space layout randomization, 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. The course can be used to satisfy the MS project requirement.

2 Course Schedule

Date	Topics	Deadlines and Remarks
Week-1 8/31	Class overview and background knowledge	
Week-2 9/7	Stack-based buffer overflow 1	Labor Day NOT Observed
Week-3 9/14	Stack-based buffer overflow 2	
Week-4 9/21	Defenses against stack-based buffer overflow 1	
Week-5 9/28	Defenses against stack-based buffer overflow 2	
Week-6 10/5	Developing Shellcode 1	
Week-7 10/12	Developing Shellcode 2	
Week-8 10/19	Written Midterm and Review	
Week-9 10/26	Format string vulnerability	
Week-10 11/2	Heap-based buffer overflow	
Week-11 11/9	Integer overflow vulnerability	
Week-12 11/16	Return-oriented programming 1	
Week-13 11/23	Return-oriented programming 2	
Week-14 11/30	Cache side-channel, Meltdown and Spectre 1	
Week-15 12/7	Cache side-channel, Meltdown and Spectre 2	In-class CTF, Written Final

Table 1: Tentative Class Schedule: 1 session per week

2.1 Rules

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

3 Grading Policy

Area	No. Items	Points per Item	Points for Area
Exams			200
Written Midterm	1	100	
Written Final	1	100	
Homework	14	45	630
In-class CTF	1		200
Attendance	14	2	28
Total			1058

Table 2: 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
Academic Dishonesty	>F<

Table 3: Final Letter Grades

4 Prerequisite

This class will be self-contained. However, solid background from the following classes helps significantly.

1. CSE 521 Operating Systems

5 Related Classes Offered by Other Professors

1. Software Security. Adam Doupe. Arizona State University. `https://adamdoupe.com/teaching/classes/cse545-software-security-s18/`.
2. Cyber Attacks and Defense. Yeongjin Jang. Oregon State University. `https://cand-f18.unexploitable.systems/`.
3. Special Topics in Software Security. Bill Harris. Georgia Tech. `https://www.cc.gatech.edu/~wharris/cs_8803.html`.

4. Software Security. Yajin Zhou. Zhejiang University. http://yajin.org/ssec2020/.

6 Plagiarism and Cheating

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, 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 plagirism behaviors.

7 Syllabus Update

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