CSE 523 - Systems Security

Learning security through hands-on experience

Spring 2022 Syllabus

Part 1: Course Information

Instructor Information

- **Instructor:** Patrick Crowley
- **Office:** McKelvey 2039
- **Office Hours:** Office hours will be held online. Please see Canvas for specific times and links.
- **How to reach me:**
    - **Course-related communication:** Please use **Piazza** for all course-related communication. General questions about the materials should be posted publicly. Personal course-related questions can be posted privately. Instructions on how to sign up for the course Piazza page will be provided in the first module.
    - **Other:** pcrowley @ wustl.edu
    - **Response time:** I will try to respond as soon as I can, but it can sometimes take me 24-48 hours to respond to your private questions. For faster response time, please include the TAs in your posts or post your questions publicly. Other students may be able to help!

Course Description

- This course examines the intersection between computer design and information security. While performance and efficiency in digital systems have improved markedly in recent decades, computer security has worsened overall in this time frame. To understand why, we will explore the role that design choices play in the security characteristics of modern systems. Students will use and write software to illustrate mastery of the material. Projects will include identifying security vulnerabilities, exploiting vulnerabilities, and detecting and defending against exploits.

Prerequisite/Corequisites

- CSE 361S is a prerequisite, although not enforced. Ideally, students should be familiar with C/C++, python, gdb, and Linux tools. The course provides pointers to online resources when additional background is needed.

Textbook & Course Materials

- **Required Text(s):**
    - Computer Security: A Hands-on Approach 2nd Edition by Wenliang Du.

- **Recommended Texts & Other Readings:**
    - Hacking: The Art of Exploitation, 2nd Edition by Jon Erickson
    - Other reading pointers will be made available through Canvas.

Online Course Structure

This is a fully-online course, although we plan to transition to in-person classes as soon as University policies permit. All course activities and resources can be found through Canvas. We will use Piazza to discuss course materials and answer questions. At designated times throughout the semester, we will participate in a blend of self-paced activities using Canvas, such as discussion forums.

Important Note: This syllabus, along with course assignments and due dates, are subject to change. It is the student's responsibility to check Canvas and Piazza frequently for corrections or updates to the syllabus. Any changes will be clearly noted in the course announcements.

Part 2: Student Learning Outcomes & Objectives

Student Learning Outcomes

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

- Understand and discuss security-related updates, as well as recent academic literature.
- Identify known software vulnerabilities, such as buffer overflow, format string, and race conditions.
- Exploit known software vulnerabilities and construct attack vectors using the techniques learned in class.
- Use penetration testing and other tools to find and auto exploit vulnerabilities (fuzzing).
- Take repeatable notes so others could reproduce your work.
- Develop security awareness and the capability to discuss the security implications of new vulnerabilities and threats.

Part 3: Topic Outline/Schedule

A typical week in the course will consist of a lecture and a lab. On most weeks, all weekly materials will be published by **10:00 am on Mondays**. We encourage you to follow the published course times, watch lectures on Mondays, and complete labs by the end of class time on Wednesdays. All the learning activities can be completed in your own time as long as they are completed by the deadlines shown in the course schedule. Class time on Wednesdays will be reserved for synchronous Q&A sessions, with some weeks reserved for synchronous lectures. During Q&A sessions, we will answer questions related to this week's materials and/or lab, and help students debug their work. We encourage you to submit your questions in advance so we can better prepare for this session, and identify common issues. Questions asked in advance will be priorities, and their answers will be recorded.

If uploading or accessing recorded materials on Canvas becomes an issue, or if we think that live lectures would work better for some course modules, then we will shift to broadcast lectures via zoom. In such cases, broadcasted lectures will be recorded and attendance will not be required.

The last two weeks of the semester are reserved for student presentations. Each student will be asked to present once throughout the semester. Presentations will be uploaded to discussion boards on Canvas, and students will be asked to comment on presentations to earn participation points.

Week #	Topic	Reading	HW	Monday		Wednesday	
1	Welcome	None	HW1 assigned			Jan 19	Lecture
2	Security Principles + Intro to exploitation	See Canvas module	HW1 due	Jan 24	Lecture	Jan 26	Studio
3	Buffer overflow - fundamentals	p. 63-79	HW2 assigned	Jan 31	Lecture	Feb 2	Studio
4	Buffer overflow - ret-to-ret	p. 80-98		Feb 7	Lecture	Feb 9	Studio
5	Buffer overflow - return-to-libc	p. 101-130	HW2 due	Feb 14	Lecture	Feb 16	Studio
6	Responsible disclosure	None		Feb 21	Lecture	Feb 23	Studio
7	Shellshock	p. 48-61	HW3 assigned	Feb 28	Lecture	Mar 2	Studio

8	Race condition & Dirty cow	p. 155-182 (skim)		Mar 7	Lecture	Mar 9	Studio
9	SPRING BREAK			Mar 14		Mar 16	
10	Metasploit	See Canvas module	HW3 due, HW4 assigned	Mar 21	Lecture	Mar 23	Studio
11	Format strings / sql injections	TBD		Mar 28	Lecture	Mar 30	Studio
12	Fuzzing	See Canvas module	HW4 due	Apr 4	Lecture	Apr 6	Studio
13	Network vulnerabilities	See Canvas module	HW5 assigned	Apr 11	Lecture	Apr 13	Studio
14	Student presentations	None		Apr 18		Apr 20	
15	Student presentations; wrap up	None	HW5 due	Apr 25		Apr 27	

Important Note: This is a tentative plan. Refer to the course calendar on Canvas for assignments and their due dates. Activity and assignment details will be explained within each week's corresponding learning module. If you have any questions, please post them on Piazza.

Part 4: Grading Policy

Graded Course Activities

Visit the **Assignments** link in Canvas for details about each assignment listed below. Click on **Quizzes** to access quizzes and exams. Note that all HW and Labs will be submitted and graded on Gradescope.

Points	Description
25	Labs
50	5 Homework assignments with the following breakdown: • HW1 - 5 points • HW2 - 10 points • HW3 - 10 points

	• HW4 - 10 points • HW5 - 15 points
15	Student Presentation(10 points) & participation (5 points)
10	Canvas quizzes
100	**Total Points Possible**

Late Work Policy

Be sure to pay close attention to deadlines. Each assignment will get a free 12-hour extension to accommodate different time zones. Example: If homework 1 is due by midnight (CST) on Wednesday, you can submit it by noon (CST) on Friday without penalty. Work submitted after the 12-hour windows will not be accepted.

Regrade requests

Points you receive for graded activities will be posted to the Canvas Gradebook. You will get a week from the time grades were posted to ask about your work or submit a regrade request. Regrade requests will not be accepted after that time. Example: If grades for HW1 were posted on Friday morning, you will have until Thursday at midnight to post your questions or submit regrade requests.

Lab Coupon

You can use up to one lab coupon throughout the semester. Hence, you can submit 9/10 labs without any penalty to your grade. If you submit all 10 labs, we will drop the lowest score.
Note 1: There is **no** free coupon for HW assignments.
Note 2: A few homework assignments rely on tasks completed in the Labs. You are responsible to make up any missed lab, regardless of your decision to not submit it.

Presentation requirements:

I will create a discussion board for each of the presentation days. Each discussion board will open at midnight, and your presentation should be uploaded to this board by 2:00 pm CT (no free extensions to upload your presentations will be given).

- Each presentation should be somewhere between 15-20 minutes.
- Slides are highly encouraged but not required.
- You must include your face in the recorded video.
- A typical presentation should include:

- (MUST) A quick introduction and necessary background of the topic (high-level description)
- The threat model/ security goal/ mechanism
- Evaluation criteria, rationale, and results (relevant for research papers)
- (MUST) Your own opinion on the topic
- (MUST) An open-ended question for discussion.

Part 5: Course Policies

Attendance Policy

There is no attendance requirement this semester except for required synchronous lectures (see course schedule). Please contact the instructor if your timezone makes it complicated to attend the synchronous lectures. Students are encouraged to attend the synchronous Q&A times but are not required to do so.

Participation Policy

Students are expected to present on a security topic of their choice and participate in the followup discussions to earn participation points.

Build Rapport

Please let us know if you find that you have any trouble keeping up with assignments or other aspects of the course, and please do that as early as possible. Make sure that you are proactive in informing us when difficulties arise during the semester so that we can help you find a solution.

Complete Assignments

All assignments for this course will be submitted electronically through Canvas unless stated otherwise.

Collaboration policy:

You **are allowed** to work with other students enrolled in the course while working on labs, and a few labs will allow group submissions (check Canvas for specifics). If you choose to submit a joint lab, you must clearly state the student names whom you collaborated with.

You are **not allowed** to collaborate with others on **homework** assignments. You are expected to complete homework assignments on your own without discussing your solutions or approach

with others.

Note that relying on other people's work, or submitting materials published in previous semesters, or completed by a student who took the course in the past is considered a violation of academic integrity.

Part 6: Technical Requirements

- You will need a computer with a stable Internet connection, a webcam, and a microphone. Students needing financial assistance to acquire the necessary hardware should contact the Office of Student Success.
- Your computer must be capable of running multiple VMs.
- If you will be based overseas, there may be technology access considerations. Contact your instructor if you have persistent issues accessing the course online resources.
- Synchronous class sessions and office hours will be conducted using Zoom. Please connect to Zoom from the Zoom page in Canvas. Both upcoming Zoom sessions and recordings of previous sessions will be available on that page. These sessions are intended for use by current students only and neither meeting invites nor recorded sessions should be shared or posted elsewhere for any purpose.
- Persistent technical issues should be worked out through the WashU Tech Den at https://techden.wustl.edu/support-help/.
- Course Software – Below are guides and resources for specific software you will likely be using in your courses:
    - Canvas: https://mycanvas.wustl.edu/studentsupport/ (this includes information on 24/7 Canvas support).
    - Zoom: https://teachingcontinuity.wustl.edu/strategies-for-learning-remotely/tips-for-using-zoom-for-class/
    - For information on how to use VPN to connect to Engineering academic lab shares or other network access to computers on campus, visit the Engineering IT Networks & Remote Access page.

Ask a Librarian: Lauren Todd, the subject librarian for engineering, is available to help with all your library and research needs. She offers virtual research help via email or one-on-one Zoom consultations. She can help you find appropriate databases and evaluate your sources. She also provides assistance with off-campus access to the library and has tips to make your research process easier. You reach her via email at lauren.todd@wustl.edu or make a Zoom appointment here. For general guidance on Engineering Research, see Research Guides.

For information on Library current operations and response to the COVID-19 outbreak, visit https://library.wustl.edu/about/covid-19/ .

Engineering Communication Center – In the Engineering Communication Center, our faculty

members offer one-on-one assistance to undergraduates, graduate students, faculty, and alumni with written, oral, and graphic communications. To schedule an appointment, visit https://wustl.mywconline.com.

For more information, contact us by email at ecc@wustl.edu.

Part 7: Academic Integrity

(From Undergraduate Programs catalog, p. 16):
"You are expected to maintain the highest standards of academic integrity and refrain from the forms of misconduct spelled out in the University Academic Integrity Policy, which is published in full in Bearings and elsewhere. Violations will lead to disciplinary action and may result in suspension or expulsion from the University.
Students and faculty have an obligation to uphold the highest standards of scholarship. Plagiarism or other forms of cheating are not tolerated. When a student has violated the standards of the academic community, an instructor may recommend that the student be brought before a disciplinary committee. These are the most frequent areas of violation:

- failure to use adequate means of documentation in written reports or essays, resulting in plagiarism
- unpermitted use of either prepared notes or the work of other students while taking a test
- alteration of test materials that are submitted for regrading
- collaboration with other students in preparing assignments, when not approved by the instructor.

Findings of academic misconduct may result in a written reprimand, failure of an assignment or course, disciplinary probation, withdrawal of merit-based scholarship support, or other sanctions. Severe or repeat offenses may be referred to the University Judicial Board for consideration of suspension or expulsion."

To be clear, you are not allowed to use, in part or in full, materials from previous offerings of this course.
Visit https://students.wustl.edu/academic-integrity/ for more on the university policy.

Part 8: Disability Resources

Students with disabilities or suspected disabilities are strongly encouraged to bring any additional considerations to the attention of the instructor and make full use of the University's Disability Resource Center (http://disability.wustl.edu).

Part 9: Title IX Statement

From Washington University statement on new Title IX rules:

“Washington University is firmly committed to addressing and preventing sexual misconduct on our campuses. Our highest priority has been and remains the safety and well-being of all of our students, faculty and staff and, as always, we will do all we can to create a safe and supportive environment for them. We will review the U.S. Department of Education’s newly released Final Rule under Title IX of the Education Amendments of 1972 and engage with members of our community in the coming weeks and months regarding implementation of any measures that may be required by changes to the law. We are determined to maintain our focus on prevention and education, fair processes and providing support to all of our community members as we review and implement the amended regulations.”

Please refer to this website for more information.