CSE227: Graduate Computer Security **Winter 2025**

Term Project

Project Intention Form Due: January 17th 11:59pm PT
Project Midpoint Check-in Due: February 14th by 11:59pm PT
Final Writeup Due: March 18th Anywhere on Earth (AoE)

Introduction

Over the course of the quarter, you will work in groups of 3–4 to conduct original research in the area of computer security.

This document will discuss the expectations and major checkpoints for this assignment, as well as provide you with rough guidelines on how to conduct open-ended research in this area. This project and its constituent parts are worth 75% of your grade in the course.

Forming a Group

Projects should be conducted in teams of 3–4 students. You can choose to work with whoever you like in the class—there are no pre-assigned groups. You can use our open Piazza thread to find groupmates: `https://piazza.com/class/m5e3ck8k5ii3lq/post/5`.

If you would like to work alone, you must meet with Deepak in advance to get this approved. There must be a very good reason for wanting to work alone—part of the learning objective for this course is working collaboratively on research.

Project Expectations

Although every project will be very different in topic, method, and execution, *all* projects will need to meet the same expectations. There are:

- Come up with a research idea area relevant to computer security in some way
- Read and synthesize related papers to the topic area
- Create a research plan that details the hypotheses, data, tests, systems, designs, or other research effort required to complete the project
- Identify how to define whether the project was successful (this should be more specific than simply "I finished the project.")
- Execute the research plan

If you are already conducting research in this area with a faculty member on campus and wish to use your ongoing research as a part of your course requirements, please discuss this with me in advance of submitting your project intention form. The scope of your work for the quarter should be **explicitly stated** at the top of the quarter so we know how you will be evaluated.

In addition to finding a project area you are interested in, students will also be asked to tag their project as either 1) offensive security research, 2) defensive security research, or 3) measurement / empirical research. These definitions are as follows:

- **Offensive security research:** Research that primarily focuses on the design and implementation of a new *attack* against an existing system or service.
- **Defensive security research:** Research that focuses on a system or defense against a novel attack in a real computer system.

- **Measurement / Empirical research:** Research that *measures* a security phenomenon by collecting data on the topic and analyzing that data to provide more insight.

A word on ethics: When conducting research, you may be inclined to try your techniques on live systems or in the real world. Those techniques may violate the law or university policy, and *worse*, they may be unethical. Under some circumstances, even probing for vulnerabilities could result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in CSE 227 is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." If you have any questions, reach out to course staff before doing something—better safe than sorry.

Milestones

There are four main milestones for this project: a project intention form, a project midpoint check-in document, a final presentation, and a final document. Each is detailed below:

Project Intention Form (10%)

This form is worth 10% of your project grade. It commits you to a group in the class and sets the main direction for your project. You can find the project intention form here: https://docs.google.com/forms/d/e/1FAIpQLSfOwIsfwxf5-Q2fdVc4bm786Ik2rhEio5KTr2Pw5RslLCOhBQ/viewform. This is due by **January 17th at 11:59pm PT**.

Midpoint Check-in Document (15%)

This 2-page document is worth 15% of your overall grade and describes your current status on the project. This will serve as an opportunity for you to describe what you have done so far. The structure of everyone's documents may vary, but the sections that **must** be included are:

- An introduction which frames the problem you are studying
- A related work section detailing prior work related to your topic
- The research plan and what your current status is for accomplishing your research goals

You should use the USENIX Security Overleaf template for this document: https://www.overleaf.com/latex/templates/usenix-2023/hhvnskcxstwq. Failure to do so will result in a 3% reduction of your overall grade. This document will also serve as the baseline for our midpoint check-in conversation which will happen at some point the week of *February 17th.* This document due by **February 14th at 11:59pm PT**.

Final Presentation and Writeup (50%)

Students will be required to put together a 10 minute presentation on their projects, to be presented in the last week of the quarter (and potentially the finals period as well, depending on student enrollment). The presentation will be followed by a question & answer session of approximately 3 minutes, depending on how many groups need to present. This presentation is worth 25% of your overall grade. You will be graded based on clarity of presentation, the rigor of your research project, and how well you handle audience questions. A more concrete rubric will be shared closer to the presentation week.

After the presentation, you will put together a 5-page document which details the progress you made over the course of the project. This report is worth 25% of your overall grade. The details of this document will vary from team to team, but the sections that **must** be included are:

- An introduction which frames the problem you are studying and the topline findings of your work
- A related works section which details the prior work related to your topic

- A methodology section which discusses how you set out to answer your research question
- A results section which documents your findings
- A discussion and future work section which puts your findings in the context of prior work, and details what future work might exist in this area.

Conclusion

Ultimately, this project should help you get exposed to conducting original research in computer security. The course staff are available by appointment to discuss your ideas and help you to frame and shape your work as necessary. Have fun!