# CPS 585 – Secure Software Systems
# Spring 2024

(Last Modified: March 19, 2024)

## 1 General

**Course**

| | |
|---|---|
| Lecture | Tue/Thu 3:05-4:20pm |
| Discussion | None |
| Location | LSRC A247 |

**Instructors**

| | |
|---|---|
| Name | Matthew Lentz |
| Email | mlentz@cs.duke.edu |
| Website | https://www.cs.duke.edu/~mlentz |
| Office Hours | Thur 11am-12pm (LSRC D314) + After Lecture |

**Resources**

| | |
|---|---|
| Website | https://courses.cs.duke.edu/spring24/compsci585 |
| Canvas | https://canvas.duke.edu/courses/27439 |
| Ed | https://edstem.org/us/courses/50540/discussion/ |
| HotCRP | https://duke-585s24.hotcrp.com/ |

## 2 Overview

This course will focus on architectural approaches to designing and building secure and trustworthy software systems, motivated by a discussion of threat models and vulnerabilities exploited in practice. We will analyze various enabling mechanisms (e.g., virtualization, trusted hardware) in terms of their abstractions, implementations, security guarantees, and hardware-software decompositions. We will survey systems that have leveraged such approaches across a wide range of application scenarios. Towards the end of the course, we will also consider other approaches to improving the security of software systems (e.g., program verification). This course will be primarily driven by reading research papers, with in-class presentations and discussions, and will include a research project component.

## 3 Expectations

### 3.1 Preconditions

The prerequisite for this course is either: 1) you are a graduate student in CS or ECE, or 2) you have completed CPS 310 (Operating Systems). Therefore, we expect that you already understand the basics of computer architecture and operating systems, and that you have experience in implementing non-trivial systems projects.

Note that while having background knowledge in computer security and cryptography is helpful, it is *not* necessary. As part of this course, we will be discussing security threats, how to formulate and reason about threat models, as well as cryptographic primitives that we will apply (and see applied) in practice.

### 3.2 Postconditions

The primary goal of this course is to prepare you for research broadly at the intersection of systems and security, with a particular focus on architectural approaches to designing and building secure software systems.

After completing this course, we expect you to be able to:

1. Read and understand research papers at the intersection of systems and security
2. Formulate and execute on an original research problem at the intersection of systems and security
3. Understand the broad landscape of approaches to improving the security of software systems
4. Understand enabling architectural mechanisms for building secure systems (e.g., trusted hardware), including their design choices, implementations, and limitations
5. Understand how architectural approaches are leveraged across a variety of application scenarios (e.g., web browsers)

## 4 Resources

**Textbooks** There are no required textbooks for this course. Papers (and other various resources) will be provided to you throughout the semester.

**Canvas** We will be using Canvas for managing project submissions and course grades.

**Ed** We will be using Ed to serve as a discussion forum for the course and the primary place for making course announcements.

**HotCRP** For accessing the readings and posting responses, we will be using the HotCRP online conference tool. Some of you may already be familiar with this tool, since it is used to manage the submission and reviewing process for many of the academic conferences in computer science (especially for systems and security areas).

## 5 Grading

Your final grade in the course will be determined by the following percentage allocations:

| **Type** | **%** | **Description** |
|---|---|---|
| Project | 45 | A semester-long research project, with writeup and presentation |
| Responses | 20 | Writing thoughtful responses to the weekly readings |
| Exam | 20 | A take-home midterm exam |
| Participation | 15 | Actively engaging with in-class and online discussions |

Note that attendance is not mandatory; however, we strongly encourage it since one of the primary aspects of this class revolves around the discussion component. You are responsible for all material covered and assignments given out during any class that you miss.

### 5.1 Project

The most significant part of this course is centered around a semester-long research project. This project should give you experience working on research at the intersection of systems and security. While we will have some general directions to help with your thinking, it is your responsibility to pick a problem to work on. By the end of the course, you will hand in a writeup similar to that of a workshop (or conference) paper as well as giving an in-class presentation on your work. It would be great to see some conference submissions emerge from this course, and I would be happy to work with you after the semester to make that a reality.

You may form your own groups of 3-4 students. Due to the size of the class, there is no opportunity for working on projects individually. Feel free to use the Ed discussion forum to advertise / find groups.

The project will be broken down into several different stages so that we can provide useful feedback throughout the semester and to ensure forward progress. The stages are as follows:

1. **Project Team [Due 01/25]:** Email me the list of 3-4 group members for your project along with your group name (optional).
2. **Project Proposal [Due 02/20]:** A 2-3 page PDF document for proposing your project. It should include the following elements:
   - Problem description
   - Background and related work
   - Approach to solving the problem
   - Plan to evaluate your solution
3. **Project Status Report [Due 03/21]:** A 1-2 page PDF document that describes the current status of your work towards completing the project. It should include the following elements:
   - Current progress
   - Previous and current blockers
   - Adjustments to proposed plans (if any)
4. **Project Presentation [Due 04/11 and 04/16]:** A 10-12 minute in-class presentation followed by Q&A from the audience.
5. **Project Writeup [Due 04/16]:** A 6-8 page PDF document in the form of a workshop or conference submission. It should ideally be typeset using LaTeX (e.g., via Overleaf). It should include the following elements, but you have some freedom with respect to the exact organization:
   - Abstract: Summarize your project
   - Introduction: Motivate the problem and your solution
   - Background and Related Work: Place your project in context
   - Design and Implementation: Describe your approach, solution, and *necessary* implementation details
   - Evaluation: Present and explain your results
   - Conclusion: Conclude and discuss future work
   - References

Unless otherwise stated, you should submit all of your deliverables through the Duke Box available via Canvas.

## 5.2 Reading Responses

Each student should individually submit responses to the readings before each class session. *Responses for papers are due by 11:59pm ET the day before the class in which they will be discussed*; for instance, if we will be discussing a paper on Tuesday, please submit the response by 11:59pm ET on Monday. This gives me a chance to read through all of your responses and determine how to focus some of the discussions during class. You will submit your responses via HotCRP, as mentioned in the "Resources" section.

*Responses should be roughly two paragraphs for each paper.* While there is no strict format for these responses, you can think about how you might describe each paper to a colleague. For instance, you might consider talking about: 1) the problem they are trying to solve, 2) the key insight(s) to address the problem, 3) assumptions and design choices, 4) how well the idea was executed and evaluated, and 5) aspects that you really enjoyed (or had issues with).

I will drop the three lowest scores on the reading responses.

### 5.3 Exam

There will be a single take-home midterm exam with no final exam. We will distribute the midterm exam on 02/22 and it is due back on 02/29. The questions on this exam will focus on lecture content and papers that we have discussed from all classes prior to 02/22.

### 5.4 Late Policy

We expect you to turn in your work by the day and time it is due. Note that if a time is not listed, you can assume the deadline is 11:59pm ET on the day listed. The only exceptions to this are based on the Class Attendence and Missed Work Policy, which you can find here: https://trinity.duke.edu/undergraduate/academic-policies/class-attendance-and-missed-work.

### 5.5 Regrading Policy

All regrading requests (responses, exams, projects) must be submitted within one week of the graded item being returned/available. Requests after one week will be denied. Please submit your request via email to me.

## 6 Academic Integrity

We expect everyone to uphold the Duke Community Standard, which you can find here: https://studentaffairs.duke.edu/conduct/about-us/duke-community-standard. In particular, this standard is comprised of:

- I will not lie, cheat, or steal in my academic endeavors
- I will conduct myself honorably in all my endeavors
- I will act if the Standard is compromised

Please ask me if you are unsure which actions may (or may not) violate the community standard as part of this course. However, you can find specific collaboration guidelines for different types of coursework below.

### 6.1 Collaboration Guidelines

**Reading Responses** You are more than welcome to discuss papers with other students; however, I expect you to each author your own responses to the papers. You should not rely on any other resources besides the paper itself.

**Exam** You are not allowed to collaborate on the take-home exam; however, you may post public *clarification* questions on the Ed discussion forum. You should only use the materials from the lectures (e.g., papers, slides, notes) and no other resources.

## 7 Students with Disabilities

Duke University is committed to providing equal access to students with documented disabilities. Students with disabilities may contact the Student Disability Access Office (SDAO) to ensure your access to this course and to the program. There you can engage in a confidential conversation about the process for requesting reasonable accommodations both in the classroom and in clinical settings. Students are encouraged to register with the SDAO as soon as they begin the program. Please note that accommodations are not provided retroactively. More information can be found online at access.duke.edu or by contacting SDAO at 919-668-1267, SDAO@duke.edu.

## 8 Environment

Interactive discussions are one of the key components that make this type of course useful, especially when we dive into more advanced topics. We want everyone to make sure that they do their best to foster an inclusive environment, since that will enable us to have the richest discussions. In general, please treat teaching staff and other students with kindness and respect both in class and outside of class (e.g., Ed forums). We will disable anonymous posting if we see any threatening or distruptive posts. If you feel uncomfortable for any reason, please let me know.

Let us know if you have concerns we can address regarding your safety or health. We understand that you may be facing negative reactions to stress and pressure, other personal challenges, or just the burdens of managing your life and future. Be mindful of your needs for sleep, exercise, proper food, recreation, social connection, and constructive engagement with your problems. We encourage you to take advantage of Duke resources for wellness and mental health.

## 9 Course Evaluations

Please take a moment of your time at the end of the semester to submit a course evaluation. These evaluations are incredibly useful to both us personally as well as to the department as a whole. You can provide your feedback at the following link: http://duke.evaluationkit.com/. Note that if you have suggestions for how we improve the course, feel free to reach out at any time.

## 10 Modifications

We tried to make this syllabus both correct and complete; however, we reserve the right to modify the contents of the syllabus while the course is underway. We will make sure that any modifications are clearly communicated to you with sufficient advance notice.