CPS 590.01 – Secure Software Systems
Fall 2021

(Last Modified: August 23, 2021)

1 General

Course

Time	Tue/Thur 5:15pm - 6:30pm
Location	Allen 326

Instructor

Name	Matthew Lentz
Email	https://www.cs.duke.edu/~mlentz
Email	mlentz@cs.duke.edu
Office	LSRC D314
Office Hours	Tue 4:00pm - 5:00pm (or by appointment)

Resources

Website	https://courses.cs.duke.edu/fall21/compsci590.1/
HotCRP	https://duke-sss21.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, I 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, I 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.

Sakai We will be using Sakai for course announcements, project submissions, and grades.

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.

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	19	A take-home midterm exam
Participation	15	Actively engaging with in-class and online discussions
Meet Your Prof	1	Meet with me to discuss research, future plans, or anything else

Note that attendance is not mandatory; however, I 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 I 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 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 up to three students. The more people you have in your group, the more I will expect. Note that you may choose to work on this project individually; however, in general, I'd suggest that you have at least one other partner.

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

1. **Project Team [Due 09/07]:** Email me the list of 1-3 group members for your project. Please feel free to use the class forum to help form groups.

2. **Project Pre-Proposal Presentation [Due 09/23]:** A 5 minute in-class presentation followed by Q&A from the audience. The goal is to get feedback from the class as a whole regarding the problem you want to solve and a *high-level overview* of your plan.

3. **Project Proposal [Due 09/30]:** A 2-3 page PDF document for proposing your project, taking into account feedback from the pre-proposal presentation. It should include the following elements:

   - Problem description
   - Background and related work
   - Approach to solving the problem
   - Plan to evaluate your solution

4. **Project Status Report [Due 10/28]:** 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)

5. **Project Presentation [Due 11/18 and 11/23]:** A 10-15 minute in-class presentation followed by Q&A from the audience.

6. **Project Writeup [Due 11/23]:** A 6-8 page PDF document in the form of a workshop or conference submission. It should include the following elements, although 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 links available through Sakai.

5.2 Reading Responses

Each student should individually submit responses to the readings before each class session. *Responses for papers are due by 5pm 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 5pm 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 you 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).

5.3 Exam

There will be a single take-home midterm exam with no final exam. I will distribute the midterm exam on 10/07 and it is due back on 10/14. The questions on this exam will focus on lecture content and papers that we have discussed from all classes prior to 10/07.

5.4 Meet Your Prof

One time during the semester, ideally towards the beginning, either come to office hours or schedule some other time to chat with me for 15 minutes. You should *not* use this time for purposes related to directly to the class (e.g., asking questions about a particular paper), but rather to discuss other things that you are interested in. This could relate to your research interests, future plans after completing your degree, etc.

5.5 Late Policy

I 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.

6 Environment

Interactive discussions are one of the key components that make this type of course useful. I 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. If you feel uncomfortable for any reason, please let me know.

7 Academic Integrity

I 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.

7.1 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.

Exam You are not allowed to collaborate on the take-home exam; however, you may post public *clarification* questions on the forum.

8 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.

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 me 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 I can improve the course, feel free to reach out at any time.

10 Modifications

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