Security in Emerging Computing and Networking Systems (Fall 2025)

CPSC 8580

Instructor Info

Mert D. Pesé

Office Hours: Tue 10a-11a

215 McAdams Hall

http://www.mpese.com

mpese@clemson.edu

Course Info

Prereq: Bachelor degree in Computer Science or equivalent

Tue & Thu

3.30p-4.45p

114 McAdams Hall

TA Info

Iwinosa Aideyan

Office Hours: Tue 12-1p

`https://clemson.zoom.us/my/iaideya`

iaideya@clemson.edu

Course Description

A computing and networking system is considered emerging if it recently started getting deployed in the real-world, or is deemed promising for a wide-scale deployment in the near future. The security issues surrounding such emerging systems, however, may prevent end users from utilizing their full potential, or, even worse, may rule out the chances of their deployment in the future. Emerging systems are increasingly including Artificial Intelligence (AI) which itself is vulnerable to attacks.

In this course, we will study security challenges in these emerging systems and discuss potential solutions. The course will start with an introductory section covering general security concepts, followed by lectures on automotive security and trustworthy AI. Lectures will be accompanied by research seminars where recent papers from leading conferences will be presented by students. A certain number of papers will also be read and reviewed by the students before class time to increase active participation in the discussion of all presentations. In addition, there will be a semester-long class project. Students can work in teams of up to 4 members. Each group is expected to write a conference-style paper describing their work. Furthermore, there will also be four homework problem sets.

(Tentative) Grading Scheme

15%	Paper Review: Write a critical response for 7 papers that are presented in class. Students can choose one paper per lecture to review. Responses are due at the beginning of class as a submission to Canvas. Check the guidelines below for more information on how to write a paper review.
15%	Paper Presentation: Choose one of the papers from the reading list and prepare a 11 minute presentation. 8 minutes of your presentation should discuss details of the required paper, as well as your review of it. The remaining 3 minutes are reserved for Q&A with the audience. Since some students will have reviewed the paper in advance, we can expect some active discussion. You will receive a Google Sheet (see course schedule) that will let you choose a paper on a first-come-first-serve basis.
20%	Homework: For a better understanding of the security lectures taught in the first half of the class, there will be four sets of homework problems. They can consist of a written and coding portion.
10%	Participation: Research can only flourish when there is an active exchange of great ideas. We want to keep the class interactive and after every presentation, there will be a brief Q&A session. Feel free to add your own critique of a paper and/or to discuss the presenter's review with the audience.
40%	Course Project: A semester-long project in this course has two goals. The first goal is to help you learn more about doing research in general. The second goal is to give you the opportunity to study particular areas of security in greater detail. Therefore, you are expected to perform a substantial research project; this involves selecting an open problem, reading the related work, designing, implementing, and evaluating a solution, and presenting your results. The main deliverables will be a project presentation, as well as a project report. Presentation grades will be based on: 1) the depth in presentation (i.e., how in-depth the paper is understood, correctness of responses to questions from the audience); and 2) slides preparation (slides need to be informative with technical depth). Class project grades will be assigned based on the novelty of the design, completeness of the system implementation, and clarity in the report.

Required Materials

There is no official textbook for the class. Slides will be provided and reading materials for each topic will be assigned from research papers that are listed in the reading section below.

Paper Review Guidelines

Write a ∼600 word critical response to each required paper.

A In the first paragraph:
   1. State the problem that the paper tries to solve; and
   2. Summarize the main contributions.

B In one or more additional paragraphs:
   1. Evaluate the paper's strengths and weaknesses;
   2. Discuss something you would have done differently if you had written the paper; and
   3. Suggest one or more interesting open problems on related topics.

Your most important task is to demonstrate that you've read the paper and thought carefully about the topic.

Your paper review must include:

- Name
- Paper Number (e.g. AS1)
- The following format
  - Font: Times New Roman
  - Font Size: 12-point
  - Line Spacing: Single spaced

Learning Objectives

- Explain common software and network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms
- Describe the cost and tradeoffs associated with designing security into a product
- Analyze cutting-edge research in automotive security, as well as trustworthy AI
- Learn to critically review a paper and summarize it, as well as review and provide helpful criticism to your peers' work
- Design a research project and learn how to write a research paper

Grading Policies

All assignments should be submitted through the course website (Canvas), unless stated otherwise. Homework and Projects are due at 11:59 PM on the due date described in the assignments. Late submissions are highly discouraged. Late policy is as follows: An immediate deduction of 10% will be applied to submissions the second after the deadline. Furthermore, 15% will be deducted every 4 hours, but before 24 hours past the deadline; submissions made 24 hours or more past the deadline will not be accepted. If you feel that an error has been made in grading an assignment or an exam, you must submit a written re-grade petition within one week after the assignment or exam has been returned to you. Verbal appeals are not acceptable and grades will not be changed after the one-week period.

Letter grades are assigned according to the standard 10-point scale: The final score will be rounded up, e.g., if you receive

A	90-100
B	80-89
C	70-79
D	60-69
F	0-59

a 89.5, it will be rounded up to 90 and you will still receive an A. There will be no extra credit opportunities throughout the semester. Curving is at the discretion of the professor.

Time to Wait

Students are expected to wait for 15 minutes after the beginning of a lecture before leaving if the instructor is late and no announcement has been posted on Canvas.

Absences

As per Clemson academic policy, course instructors may use reasonable academic penalties which reflect the importance of work missed due to unexcused absences, since absence from class is detrimental to the learning process. Course instructors who penalize students for unexcused absences must state attendance requirements as related to the grading, on the course syllabus and keep accurate attendance records. See the Academic Regulations section of the current Undergraduate catalog or the Policies and Procedures of the Graduate catalog, both located at the Course Catalog home page.

If you are sick, please stay home. Let the professor know in advance via e-mail that you are not attending that day's class and you are fine. If there are other reasons (e.g., family-related, etc.) that you cannot attend, please let the professor know as well.

Academic Integrity

As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a "high seminary of learning." Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form.

See the Undergraduate Academic Integrity Policy website for additional information and the current catalogue for the policy. For graduate students, see the current Graduate School Handbook for all policies and procedures.

Accessibility

Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should let the instructor know and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen, if at all possible, but there could be a significant wait due to scheduled appointments. Students who have accommodations are strongly encouraged to request, obtain and send these to their instructors through the AIM portal as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester.

You can access further information at the Student Accessibility website. Other information is at the university's Accessibility Portal.

The Clemson University Title IX Statement Regarding Non-Discrimination

The Clemson University Title IX statement: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This Title IX policy is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX

Clemson University aspires to create a diverse community that welcomes people of different races, cultures, ages, genders, sexual orientation, religions, socioeconomic levels, political perspectives, abilities, opinions, values and experiences.

Emergency Preparation

Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees should be familiar with guidelines from the Clemson University Police Department. Visit here for information about safety.

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

1. Ensure you are signed up for emergency alerts
2. Download the Rave Guardian app to your phone
3. Learn what you can do to prepare yourself in the event of an active threat

Your Well-being is Important

As a student you may experience a range of personal issues that can impede learning, such as strained relationships, increased anxiety, alcohol/drug concerns, feeling down, sadness, difficulty concentrating, lack of motivation, or other issues. These mental health concerns may impact your academic performance or your participation in daily activities. It is very important that you ask for help when you are struggling. Please reach out to me or to Clemson's mental health services to guide you to resources that will help.

Changes to Syllabus

Lecture topics and assignments are subject to change. The course syllabus is a general plan for the course; deviations to the class may be necessary and will be announced to class by the instructor.

Ethics and Law

To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in this course 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." Understand what the law prohibits. The EFF provides helpful advice on vulnerability reporting and other legal matters.

AI Statement

The use of artificial intelligence (AI) tools are not permitted for any work in this course, even with proper documentation and citation.

Course Schedule

Date	Topic	Other Notes
08/21 (R)	Course Introduction	N/A
08/26 (T)	Lecture 1: Fundamental Concepts	N/A
	Course Project Introduction	N/A
08/28 (R)	Lecture 2: Cryptography (Part I)	HW1 released
09/02 (T)	Lecture 3: Cryptography (Part II)	N/A
09/04 (R)	Lecture 4: Network Security (Part I)	Paper Presentation Selection released
09/09 (T)	Lecture 5: Network Security (Part II)	HW1 due
09/11 (R)	Lecture 6: Software Security	HW2 released
09/16 (T)	Project Proposal Presentation	Proposal due
09/18 (R)	Lecture 7: Automotive Security (Part I)	HW2 due
09/23 (T)	Lecture 8: Automotive Security (Part II)	HW3 released
09/25 (R)	Lecture 9: Trustworthy AI - Intro and ML Basics	N/A
09/30 (T)	Lecture 10: Trustworthy AI - Adversarial Examples (Part I)	N/A
10/02 (R)	Lecture 11: Trustworthy AI - Adversarial Examples (Part II)	HW3 due
10/07 (T)	Lecture 12: Trustworthy AI - Data Poisoning	HW4 released
10/09 (R)	Lecture 13: Trustworthy AI - Membership Inference	N/A
10/14 (T)	Fall Break (No Class)	N/A
10/16 (R)	Lecture 14: Trustworthy AI - Model Extraction (Part I)	N/A
10/21 (T)	Lecture 15: Trustworthy AI - Model Extraction (Part II)	HW4 due
10/23 (R)	Paper Presentations 1	N/A
10/28 (T)	Paper Presentations 2	N/A
10/30 (R)	Midterm Project Presentations (Part I)	Midterm Report due
11/04 (T)	Midterm Project Presentations (Part II)	N/A
11/06 (R)	Paper Presentations 3	N/A
11/11 (T)	Paper Presentations 4	N/A
11/13 (R)	Paper Presentations 5	N/A
11/18 (T)	Paper Presentations 6	N/A
11/20 (R)	Paper Presentations 7	N/A

11/25 (T)	Final Project Presentations (Part I)	N/A
11/27 (R)	Thanksgiving Break (No Class)	N/A
12/02 (T)	Final Project Presentations (Part II)	N/A
12/04 (R)	Final Project Presentations (Part III)	Final Report due