Computer Security Principles (Spring 2023)

CPSC 4200/6200

Instructor Info

Mert D. Pesé

Office Hours: Mon & Wed 12-1p

215 McAdams Hall

http://www.mpese.com

mpese@clemson.edu

Course Info

Prereq: CPSC 3220 or ECE 3220 and CPSC 3600 or ECE 4380 with a C or better.

Mon & Wed & Fri

1.25p-2.15p

358 Humanities Hall

TA Info

Thomas Randall

Office Hours: Thu 2-3p

201 McAdams Hall and `https://clemson.zoom.us/j/91049909839`

tlranda@clemson.edu

Course Description

This course teaches the security mindset and introduces the principles and practices of computer security as applied to software, host systems, and networks. It covers the foundations of building, using, and managing secure systems. The four major topics of this course consist of (i) an introduction to cryptography, (ii) web and network security, (iii) host and application security, as well as (iv) examples of real-world security. Lectures include fundamental concepts and principles of software security, operating system and network security, firewalls and intrusion detection systems, private and public key cryptographic algorithms, hash functions, authentication, TLS and web security.

The knowledge obtained from lectures will be deepened by working on homework projects. Students will implement and learn about attacks and defenses that have been either discussed in the lecture or are an extension of the lecture content. As a result, students will obtain a better understanding of fundamental security concepts. Besides the homework projects, there will be two exams (one midterm and one final) and online quizzes at the beginning of each lecture to check understanding.

(Tentative) Grading Scheme

50%	Homework Projects: There will be four projects, which will count for a total of 50% of your course grade. Project teams must consist of two students. You can only team up with students from your course (e.g., a student taking CPSC 4200 can only work with another student taking CPSC 4200). Students taking CPSC 6200 will have additional assignments in each homework to work on. You may consult general reference material, but the material you turn in must be entirely your own work, and you are bound by the Academic Integrity policies of Clemson University.
40%	Exams: There will be two in-person, closed-book exams which are listed in the course schedule below. Each exam counts 20% of the overall grade. The first exam is a midterm that covers Lectures 1–20 and the second exam is a final that is cumulative, i.e., covers Lectures 1–34.
10%	Participation: At the beginning of each lecture (34 in total), there will be a short quiz on Canvas. Students will get 5 minutes at the beginning of each lecture to submit the quiz online. Students will be allowed to drop/skip 4 quizzes.

Required Materials

The official textbook for the class is "Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition" by Ross Anderson (ISBN 978-1119642787). This textbook is not required, but recommended. Slides will be provided on Canvas on the same day of the class.

Learning Objectives

- Explain basic principles and practices of computer security
- Develop a conceptual vocabulary for applied cryptography
- Explain common software and network vulnerabilities and attacks, as well as defense mechanisms against network attacks, and cryptographic protection mechanisms
- Describe the cost and tradeoffs associated with designing security into a product
- Implement and learn about existing attacks by working with a partner
- Learn about real-world security in emerging systems

Grading Policies

All assignments should be submitted through the course website (Canvas), unless stated otherwise. Homework and Projects are due at class time on the due date described in the assignments. Late submissions are highly discouraged. Late policy is as follows: An immediate deduction of 50% will be applied to submissions after the deadline 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.

* For CPSC 4200 only.

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

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.

Course Schedule

Date	Topic	Other Notes
1/11 (W)	Course Introduction	N/A
1/13 (F)	Lecture 1: Security Mindset	N/A
1/16 (M)	MLK Day (No Class)	N/A
1/18 (W)	Lecture 2: Message Integrity (Part I)	N/A
1/20 (F)	Lecture 3: Message Integrity (Part II)	N/A
1/23 (M)	Homework Setup	HW1 released
1/25 (W)	Lecture 4: Randomness & Ciphers	N/A
1/27 (F)	Lecture 5: Confidentiality (Part I)	N/A
1/30 (M)	Lecture 6: Confidentiality (Part II)	N/A
2/1 (W)	Lecture 7: Key Exchange	N/A
2/3 (F)	Lecture 8: Public Key Cryptography (Part I)	N/A
2/6 (M)	Lecture 9: Public Key Cryptography (Part II)	HW1 due
2/8 (W)	Lecture 10: Web Security - Introduction	N/A
2/10 (F)	Lecture 11: Web Security - SQL Injection, XSS, CSRF	N/A
2/13 (M)	Lecture 12: HTTPS (Part I)	HW2 released
2/15 (W)	Lecture 13: HTTPS (Part II)	N/A
2/17 (F)	Lecture 14: Networking 101 (Part I)	N/A
2/20 (M)	Lecture 15: Networking 101 (Part II)	N/A
2/22 (W)	Lecture 16: Network Attacks (Part I)	N/A
2/24 (F)	Lecture 17: Network Attacks (Part II)	N/A
2/27 (M)	HW1 & HW2 Recap	HW2 due
3/1 (W)	Lecture 18: Network Attacks (Part III)	N/A
3/3 (F)	Lecture 19: Network Defenses (Part I)	N/A
3/6 (M)	Lecture 20: Network Defenses (Part II)	HW3 released
3/8 (W)	Midterm Review Session	N/A
3/10 (F)	Midterm Exam (in class)	Covers Lectures 1–20
3/13 (M)	Lecture 21: Authentication and Passwords (Part I)	N/A
3/15 (W)	Lecture 22: Authentication and Passwords (Part II)	N/A

3/17 (F)	Lecture 23: Malware	N/A
3/20 (M)	Spring Break (No Class)	N/A
3/22 (W)	Spring Break (No Class)	N/A
3/24 (F)	Spring Break (No Class)	N/A
3/27 (M)	HW3 Recap	HW3 due
3/29 (W)	Lecture 24: Control Hijacking (Part I)	N/A
3/31 (F)	Lecture 25: Control Hijacking (Part II)	N/A
4/3 (M)	Lecture 26: Control Hijacking (Part III)	HW4 released
4/5 (W)	Lecture 27: Access Control and Isolation	N/A
4/7 (F)	Lecture 28: Digital Forensics	N/A
4/10 (M)	Lecture 29: Side Channels	N/A
4/12 (W)	Lecture 30: Privacy (Part I)	N/A
4/14 (F)	Lecture 31: Privacy (Part II)	N/A
4/17 (M)	Lecture 32: Automotive Security	HW4 due
4/19 (W)	HW4 Recap	N/A
4/21 (F)	Lecture 33: IoT Security	N/A
4/24 (M)	Lecture 34: Adversarial Machine Learning	N/A
4/26 (W)	Final Review Session	N/A
4/28 (F)	No Class	N/A
5/5 (F)	Final Exam	Covers Lectures 1-34