Syllabus

CAP 5150: Foundations of Computer Security and Privacy

Basic information

Office Title	CAP 5150: Foundations of Computer Security and Privacy
Semester	Fall 2021
Instructor	Dr. David Mohaisen (HPA2-240)
Time	Friday (2:00PM– 5:00PM)
Office Hours	Friday (11:00AM-12:00PM) – via zoom: 241 737 1400
E-mail	mohaisen@ucf.edu (preferred way of communication)
Location (lecture)	HEC-0104
Teaching Assistant	NA
Zoom	241 737 1400
Phone	407-823-1294
Graders	Dr. David Mohaisen
Textbook	No textbook is assigned.
Readings	1. Introduction to Modern Cryptography. Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC, Second Edition, 2014 2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. CRC Press, 1996 3. Introduction to Computer Security, Michael Goodrich and Roberto Tamassia, Pearson, First Edition, 2010 4. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. Michael Howard, David LeBlanc, and John Viegna. McGraw-Hill, 2005
Notes:	The topics covered on applied cryptography (first half) are mostly following Katz and Lindell's and the topics covered in computer security are partly following Goodrich and Tamassia. You do not have to buy any of those books to do well in this course, though.

Scope and Objectives

In this course, students will learn various foundational concepts in applied cryptography and computer security. Topics taught in the class and specific contents are focused on various advances in the aforementioned areas and are below. The course combines both lecture-based and project-based approaches. Semester- long projects are the major theme of this course and require a lot of hacking (details are below). By the end of this course, the students will be able to answer the fundamental question of what it means for a system to be secure. This question will be answered by reviewing the appropriate security definitions, models, mechanisms, attacks, and defenses.

Attendance Policies

Attendance of the in-class lectures is *not mandatory*, and no points are assigned to it, but students are expected to attend all lectures to perform well in the class. Notwithstanding that, no additional accommodations are provided, and recording will be available. Note that projects, assignments, and (take home) tests will be discussed only in class. All works, including projects, are to be done individually.

Assignments and Grading Policy

The following general policy is to be enforced in whole:

- **Individual works**: All assignments, quizzes, and exams in this course are to be done individually. While discussing the homework with other students is permitted, you should do your homework by yourself.
- **Exams format:** All exams are open book and open notes. Moreover, for this year's offering, all exams will be take-home and will be due in 24 hours after they are posted online. Late submissions for the exams (midterm and final) will not be graded and will automatically be given a zero grade.
- **Late submission policy for assignments other than exams and project deliverables**: All assignments will be released *sometime* on Thursday and will be due on the next Sunday, 11:59PM (see the detailed schedule below). Late submissions by at most 24 hours will be accepted and graded out of 50% of the original score worth. For example, your posted grade will be 0.5xG where G is the grade you would have obtained assuming you have submitted on time. All assignments submitted after 24 hours of the deadline will not be graded and will be worth 0%.
    - All submissions will be handled electronically with firm deadlines (i.e., being late by one second is the equivalent to being late by 24 hours). Plan your submissions accordingly.
- **Similarity scores**: given that all submissions will be handled electronically, we will use an online tool provided by the university to check similarity between the submitted answer sheet by every student and other sources, including submissions by other students, online resources, and the slides posted by the lecturer. To avoid a high similarity score, use your own words and paraphrase. Remove the questions from the answer sheet, and only provide answers in your submission. Any submission with a similarity score more than 40% with the aforementioned resources will not be graded and will be automatically given 0. *Failing the similarity test for three times in the whole semester will result in automatically failing in the course.*
- **Letter grades and curve:** We do not grade on a curve, and your grade will be independent of how others performed in this course. Adjustments will be made (e.g., dropping the lowest homework, dropping questions all or most students did not get right in an exam, minor adjustment to the distribution of grades below, etc.). The following is the distribution of letter grades (up to the next grade): A ≥ 90, B ≥ 80, C ≥ 70, F < 70.

Grade Distribution and Graded Components

The final distribution of the grade in this course will be as follows (all assignments are due on 12:00pm; that is middle of the day).

– Assignments	40% (10 assignments, each worth 4% of the total grade)	
	• Homework #1	September 9, 2021
	• Homework #2	September 16, 2021
	• Homework #3	September 23, 2021
	• Homework #4	September 30, 2021
	• Homework #5	October 7, 2021
	• Homework #6	October 21, 2021
	• Homework #7	October 28, 2021
	• Homework #8	November 4, 2021
	• Homework #9	November 11, 2021
	• Homework #10	November 18, 2021
– Midterm	20% (take home exam)	October 14, 2021 (in class)
– Project	20% (see below)	
– Attendance	0%	
– Final	20%	See the schedule online

Paper reading assignments: Assignments 3, 7, and 9 will be reading assignments. In each of those assignments, each student will be expected to read, summarize, and critique a research paper on the topics being discussed in the class. Each summary is expected to include the following aspects:

1. A summary statement: this statement should be of no less than 400 words. The summary statement should highlight the problem statement, the main technique, and the main findings of the paper. Copying the abstract or parts of the paper, as with the above similarity policy, will result in automatic 0 for this assignment. The summary statement should be nontrivial and highlight at a technical level the contribution of the work.
2. Main strengths: describe concisely 3 strengths of the technical contribution in technical terms. Each of those strengths should be no more than 100 words.
3. Main weaknesses: describe concisely 3 strengths of the technical contribution of the paper in technical terms. Each of those weaknesses should be no more than 100 words.

Papers selection: The papers will be selected as follows: divide the ***last digit*** of your student ID by 3 and find the remainder (e.g., 7/3=1; 5/3=2; 9/3=0) then add 1 to the answer and select the paper based on the outcome. (e.g., for student id 950950, the answer is 1; for student id of 950951, the answer is 2).

- The assigned papers are to be determined at a later date.

Assignments 4, 6, and 8 will be programming assignments.

All other assignments will be written assignments.

Project

A significant component of the course (20%) is a project. The project will be done by a group of exactly three (3) students. The research project should address a problem related to applied cryptography and computer security (including privacy). This may include:

- A nontrivial attack on a recently published design, or a widely used system.
- A meaningful defense against a nontrivial attack or vulnerability.
- A design of a protocol, algorithm, or system that improves security/privacy of a prior work.
- An implementation of a recently published work demonstrating previously unknown aspects of it that are equally interesting and unique
- A security analysis of a system or protocol that is not intended as a secure system (or protocol) and highlighting ways to make secure.
- Analyzing a dataset that would result in understanding behavioral traits, use patterns, etc., and can be used for applications of security and privacy.
- A survey on some recent research problem related to computer security or privacy.

Project selection. It is the responsibility of the students to select their projects and come up with a team. The instructor should be informed of the team members as soon as possible, and no later than the deadline for the project proposal. During the first week of the course, and until the deadline of the project proposal, feel free to use the instructor's office hours to discuss potential ideas and topics for the project. Before submitting the proposal, make sure that the instructor is aware and approving of the project topic (note: those are deadlines; the late submission policy for assignments applies to those deadlines; see proposal info below for more details on other avenues of getting the proposal approved via webcourse communication if you cannot make it to the office hours).

– Project proposal and team	3% (September 5, 2021)
– Project milestone	5% (October 16, 2021)
– Project presentation	6% (December 3 and December 10)
– Project report	6% (December 10)

Submissions guideline:

- Proposal: the proposal has to be up to 2 pages and must include the following information: 1) title of the project, 2) names of the team members, with a designated lead, 3) what is the problem the project tries to address, 4) what technique you expect to use for addressing the problem, 5) what outcomes you expect to get as a result. Make sure that you list each team member and what they expect to do for this project. The work distribution is important to evaluate the final project outcomes and time spent on the project against the initial tasks. The topic of the proposal has to be discussed and preapproved beforehand with the professor (via webcourse direct messages; tag all of your team members in any communication related to the project).
- Project milestone: the project milestone has to be at most 4 pages on the ACM template of 2 columns, highlighting a concise and final problem statement, technique, initial results, and initial discussion with the work distribution of team members (what each member has done and how much time they spent on such work).
- Final report: the final report has to be exactly six (8) pages + as many pages as needed for references on the ACM template of 2 columns. The final report must include the following (in order): a concise abstract, a clear introduction, a concise problem statement, related work, technique, evaluation, discussion, and conclusion.
- NOTES:
  - You are responsible for proofreading everything you deliver for this course project. Typos will not be tolerated.
  - Quality of presentation and writing is expected, and last-minute work won't make the cut for this class component.
  - Make sure that you spend your time wisely on the project during the semester.

Exams

The second largest component of this course is exams. In this course, you will have one "midterm" exam and one final. Both exams (combined) are worth 40% of the grade with the time as above. No make-up exams will be given, and no exceptions. No incomplete will be given in this class. Please take that into account as the important guideline when considering whether this course is right for you.

Contents and Tentative Schedule

Part I: Applied cryptography (5 weeks)

- Symmetric key cryptography (1 week): computational cryptography, computational security, pseudorandomness and associated notions, security against CPA and CCA
- Message authentication codes and hash functions (1 week): message integrity, encryption vs message authentication, CBC-MAC, collision resistance and other notions, NMAC and HMAC.
- Pseudorandom permutations (0.5 week): Feistel networks, DES and its security, AES and its security, introduction to crypto analysis
- Public key cryptography (0.5 weeks): number theory, primes, factoring, and RSA, groups and assumptions in groups, cryptographic applications of number theory
- Public key encryption (1 weeks): definitions of security and notions, hybrid encryption schemes, RSA, El Gamal, trapdoor permutations, other cryptosystems; Goldwasser-Micali, Rabin, Paillier, and ABE.
- Digital signatures (1 week): notions and definitions, RSA, hash-and-sign, Lamport's and recent applications, DSS, certifications, and PKI standards

Part II: Computer Security (7 weeks)

- Networks Security (5 weeks); Transport security: HTTPS, SSL, TLS, RPKI, BGPSEC, IPSEC, DNSSEC; Network attacks and defenses: DDoS, botnets, defenses, passwords, offline attacks, online attacks, reflectors, etc.; Application security: bugs, shellcodes, viruses, worms, viruses, spyware; Web security: cookies, tracking, XSS, SQL injection, defenses; Advanced threats: cyber warfare and APTs

- Privacy and Ethics (2 weeks): TOR, OTR, GPG, anticensorship, and ethical considerations.

General Policies and Accommodations

Take a moment to familiarize yourself with the following university-level policies:

- Classroom responsibility
- Non-discrimination policy
- Religious observances
- Sexual harassment policy
- Special accommodation policy: The university provides an ample of resources to enable the inclusion of students with different needs. Common academic accomdations available at the university include alternative testing, course notes, accessible technology, alternative formats, speech-to-text captioning, ASL interpreting, course attendance, and other accommodations. Please take a moment to familiarize yourself of what is available as a special accommodation. In particular, I am committed and glad to help with reasonable accommodations for disabilities. The procedure is outlined in the following statement (quoted from the faculty center for teaching and learning's web site):
    - "The University of Central Florida is committed to providing reasonable accommodations for all persons with disabilities. This syllabus is available in alternate formats upon request. Students with disabilities who need accommodations in this course must contact the professor at the beginning of the semester to discuss needed accommodations. No accommodations will be provided until the student has met with the professor to request accommodations. Students who need accommodations must be registered with Student Disability Services, Student Resource Center Room 132, phone (407) 823-2371, TTY/TDD only phone (407) 823-2116, before requesting accommodations from the professor."