Computer Security
CMPS 122

Dr. Karim Sobh
Computer Science Department
Jack Baskin School of Engineering
ksobh@cs.ucsc.edu

Spring 2017

Basic Information

- **Course Title:** Computer Security (CMPS 122)
- **Prerequisites:** Introduction to Computer Engineering (CMPS 111)
- **Lectures:** TuTh 09:50 AM - 011:25 AM (PhysSciences 140)
- **Instructor:** Dr. Karim Sobh (ksobh@ucsc.edu)
  Office Hours: 12:00 - 13:30 TuTh (E2-255)
- **TA:**
  Karthik Mohan Kumar (kmohanku@ucsc.edu)
  Office Hours: Mon 10:00 - 11:30 AM, Wed 11:00 AM - 12:00 PM (E2-480)
- **Labs:** A set of pre-scheduled sessions performed by the TA, and locations as well as different dates and times will be communicated with the students.
- **Home page:** `https://cmps122-spring17-01.courses.soe.ucsc.edu/`
- **Discussion:** `https://piazza.com/ucsc/spring2017/cmps122`

Catalog Description

Introduction to computer security, covering main fundamentals of Network Security, Access control, Security in programming languages, Basic cryptography, Security protocols, Authentication, and Different types of security attacks.

Textbooks and References

- William Stallings, and Lawrie Brown. Computer Security: Principles and Practice, 3rd Edition, 2015, Pearson Education, ISBN: 978-0-13-377392-7. **(MAIN)**
- Al Sweigart. Hacking Secret Ciphers with Python: A beginner's guide to cryptography and computer programming with Python, April 14, 2013, CreateSpace Independent Publishing Platform, ISBN: 978-1482614374.
- Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, April 2008, John Wiley & Sons, ISBN: 978-0-470-06852-6.

Course Goals

1. Introduce fundamental computer security concepts.
2. Exposure to broad width of security against different domains of computing.
3. Understand the theory and the evolution of important security concepts, e.g. cryptography.
4. Understand the difference between different security attacks.
5. Ability to use security attacks counter measures in the appropriate context.
6. Hands-on implementation experience with selective algorithms and protocols.
7. Ability to modify and amend operating system security modules.
8. Conduct relatively special literature review in different security topics.

Major Topics Covered

- Cryptography.
- Internet Authentication.
- Public Key Infrastructure (PKI).
- Buffer Overflow.
- Web Applications Security.
- Malicious Software.
- Network Security.
- Denial of Service Attacks.
- Intrusion Detection.
- Intrusion Prevention and Firewalls.
- User Authentication.
- Operating System Security.

Exams

Students must attend all exams, the midterms and the final. The final is a comprehensive exam with emphasis on material that were not covered in the mid-term. In case of absence due to emergency, the student needs to let the professor know before the scheduled exam date. Moreover, the student will be required to present a legitimate justification as proof such as a **doctor's note or letter from the funeral home** before taking a makeup for the exam.

Assignments

Through out the course duration, students are required to work individually on 3-4 assignments. Moreover, a survey paper is due near the middle of the second half of the quarter, and students can work on it in groups of 2-3. Each group will be required to submit a paper and give an in-class 20 minutes presentation showcasing the most important contributions of the survey. The students can choose the topics, but topics will need to be approved by the professor.

Each assignment will have a due date that will be announced with the assignment, and late submissions of the assignments will result in a deduction penalty of 10% per day, with a maximum of 5 late days (including holidays, and week-ends) after which the assignment will not be accepted. With the same concept, assignments submitted earlier than the deadline will be credited 1% for every 12 hours (half-day), with a maximum of 10% credit. The maximum grade that the student can attain is 100% irrespective of how early an assignment is submitted.

It is highly recommended to start immediately, and as early as possible, as assignments will require time to complete as per requested. Each assignment can only be submitted once, and should have all the needed information that will help the grader evaluate the work such as code, in-code documentation, explanation of the design approach and reasons why specific routes were taken, etc. Simply, it is the responsibility of the student to showcase his/her work.

More details about the assignments will be available towards the beginning of the quarter.

Notes and Class Participation

Students are required to take notes and participate in class. Part of the grade is attributed to how active the student is. Weekly notes must be turned in on eCommons latest by Sunday 9 PM of the week after the material was covered. The notes can be hand written or typed by **the student**, and they should not be copied form textbooks, class slides, other students, or the internet.

There are many forms of participation, mainly class attendance, actively participating in class discussions, visiting course staff during their office hours, and/or participating in the piazza discussion. The student is encouraged to perform all of these as it is of great benefit to the student and might enhance the final grade.

Grading

The course overall grade is split over two components; exams and assignments. A student needs to get at least 50% of the total grade of each component to pass the course; Each component needs to be passed. For example the following cases will definitely fail the course:

- Scoring 55% in the exams and 51% in the assignments.
- Scoring 100% in the exams and 30% in the assignments.
- Scoring 28% in the exams and 90% in the assignments.

The final grade will be calculated as follows:

- Homework Assignments: 30%
- Survey Paper: 20%
- Midterm Exam: 20%
- Final Exam: 25%
- Participation & Attendance: 5%

The following are tentative approximate ranges of the overall scores:

- A: 89-100%
- B: 79-89%
- C: 69-79%
- D: 60-69%
- F: below 60%

Individual exams, or assignment can be curved based on the situation and the overall distribution of the grades. Also, extra bonus work might be offered near the end of the course based on the grades distribution but with no guarantees.

Attendance

Students are required to attend the lectures. Exam questions will be designed to refer to lecture discussions and examples, and will require knowledge of specific details discussed in the lectures. Students failing to attend the lectures have a high chance of loosing marks on the exams. By not attending the lectures the student will also find it difficult to take good notes. Lab section attendance is not required, although important material on the programming projects will be missed if the student does not attend, since that will be where projects will be discussed in detail.

Getting Help

The student is advised to always ask for help as early as possible and not to wait. One way of getting help is through engaging in informative discussions with the course staff during their office hours. However, for these discussions to be fruitful the student should:

- Attend classes and lab sections.
- Read the course Web page for information on assignments.
- Read and post to the class discussion forum, hosted at piazza.com

The student should try to avoid dropping by outside the office hours as the course staff might be busy and might not be able to avail the time to help at the time. If the student cannot attend office hours, the student should arrange a meeting in advance by emailing the person he/she would like to meet with. Questions can also be posted to course staff via email as long as they can be replied to in short answers.

Students with Disabilities

UC Santa Cruz is committed to creating an academic environment that supports its diverse student body. If you are a student with a disability who requires accommodations to achieve equal access in this course, please submit your Accommodation Authorization Letter from the Disability Resource Center (DRC) to me privately during my office hours or by appointment, preferably within the first two weeks of the quarter. At this time, I would also like us to discuss ways we can ensure your full participation in the course. I encourage all students who may benefit from learning more about DRC services to contact DRC by phone at 831-459-2089 or by email at drc@ucsc.edu for more information.

Academic Honesty

Academic Honesty is a very important aspect in academic life. The students are expected to respect and adhere to the highest levels of academic integrity standards. There are many forms for cheating and all of them are considered a violation, which means that plagiarism is not accepted by any means. Consequently, students are not allowed by any means to do any of the following or anything similar:

1. Work on assignments with anyone.
2. Share code with anyone.
3. Share material or notes with anyone.
4. Share written class notes with peers or anyone.
5. Obtain help in assignments from anyone other than the assigned course staff.
6. Use of online past material that might help in solving the assignments.
7. Request help through online forums to help solve assignments.

If the student obtains help in any aspect of the practical work of the course the student is encouraged to document the source. In such cases it will not be considered or reported as cheating, nevertheless it might lead to a lower grade for that. So documenting the sources when turning the work in is highly advisable, as it will not count at all if it is caught afterwards.

By **anyone** we mean friends, family, former or current Computer Science students, other humans, animals, zombies, sparkling vampires, materials found on the Internet. Any cheating attempt in the assignments or the exams will result in failing the course. The Student is encouraged to read `http://registrar.ucsc.edu/navigator/section1/academic-integrity.html`. Moreover, the Academic Misconduct Policy for Undergraduates will be applied; the student should refer to `https://www.ue.ucsc.edu/academic_misconduct` for more information. The policies will be applied on all parties participating in a misconduct, both the transmitter and the receiver of the information and material in any form.

The bottom line is: do not ever cheat, or you will definitely fail the course.