CS 419: Computer Security

Spring 2023

Instructor:	Leo Fan	**Time:**	Monday 5:40 PM - 8:40 PM
Email:	xiong.fan@rutgers.edu	**Place:**	TIL-254.

Course Pages: Canvas

Office Hours:

- Leo Fan: After class, or by appointment, or send me an email. Office: Hill 264A.
- TAs: TBA.

Please include [CS419] in all email communication about course-related matters.

Recitations: Recitations will preview the laboratory released on the day of the recitation so students understand what is expected of them, and/or review the laboratory that was due the previous week and present the staff solutions, so students can receive additional feedback on their solutions.

Office hours: The TAs will hold office hours each week, both in-person and on Zoom. We will announce the time and location of office hours on Canvas during the first week of classes. Instructors will hold individual office hours by appointment.

Course Overview: This course broadly focused on computer security that covers the foundations of secure systems and cryptography. Topics covered include private/public key encryption, message authentication, digital signatures, access control, as well as network security, web security, cloud security and blockchains. This course will allow undergraduates to enter the important field of computer security earlier in their undergraduate program and also serve as an entry point for the graduate offerings.

Main References: There is no required textbook for this class. The following book are helpful:

- Introduction to Modern Cryptography, 3rd Edition, Katz and Lindell, Chapman & Hall/CRC 2020.
- Cryptography and Network Security: Principles and Practice, 6th Edition, Stallings, Pearson 2014.
- Introduction to Computer Security, Goodrich and Tamassia, Addison Wesley, 2011.

Prerequisites: Reasonably proficient in C and Unix. Basic knowledge of discrete mathematics and computer systems.

Tentative Course Outline:

- Software security: Memory safety, malware, static analysis and web security.
- Cryptography: message authentication codes, digital signatures and private/public key encryption,
- Network security: Attacks on TCP, DNS, firewalls and anonymity.
- Special topics: differential privacy, side-channel attacks, bitcoin and blockchain.

Grading Policy:

- (32%) Programming projects (about 4).
- (18%) Homework assignments (about 3).
- (25%) Midterm exam.
- (25%) Final exam.

Exams: All exams will be closed book, closed notes, no electronic devices, and please turn off cell phones. Attendance at the midterm and the final exam is mandatory and may not be excused. A midterm may be rescheduled at the emailed request. Course-wide makeup midterms will be given within a day of the scheduled date. Conflict Final Exams will be scheduled by the registrar.

Projects and homeworks: This course contains 4 programming projects and 2-3 homework assignments. Instructions will be posted on the course webpage and announced on Canvas at least one week before the due date. Projects/assignments should be submitted online via Canvas. Late submission will not be accepted without documentation supporting legitimate reasons.

- If you dispute your score on a project or homework, you must contact the TAs within one week from the date that your project/homework is officially returned.
- It is acceptable, and you are encouraged, to discuss the projects/homeworks with others, but you must do the coding and/or final write-up by yourself (unless it is a group assignment). Both copying code/writeups and allowing others to copy your code/writeups will be considered as academic dishonesty.

Academic Honesty: You are free to discuss the problem sets with others. However, the actual writeup of your assignments must be done ONLY by yourself (and without copying from notes or other sources!). In addition, you must acknowledge your sources and the discussions in your submission.

Please read the Academic Integrity Policy (`http://academicintegrity.rutgers.edu/`) for full details. If you are having trouble with the course, come speak to me!