Course Title: Computer & Network Security
Course Number: CS 433/533

Course Description

As both a science and an art, computer and network security has become one of those must-learn disciplines. This course will be comprehensive, covering both fundamental security topics and practical solutions. Yet, it is designed to be manageable for effective learning. Twenty lectures over ten weeks are designed for this class. Here are sample topics (each with a sample question):

- Elementary cryptography (what is the difference between classic cryptography and public-key cryptography?)
- Program security (why virus/worm/Trojan horses are rampant on computer and networks?)
- Protection in general-purpose operating systems (what is access control of memory/address/file/user account?)
- Designing trusted operating systems (can virtualization or layered design help secure an OS?)
- Security in networks (can a firewall deal with all network security threats?)
- Privacy (Is your email or web visits protected with good privacy?)
- Administering security (how to conduct risk analysis and design your security policies?)
- Legal and ethical issues in computer security (now that we catch an attacker, so what?)

Prerequisites

- CS 415 (Operating Systems) for CS 433

Instructor

- Prof Jun Li
- Email: `lijun@cs.uoregon.edu`
- Office hours: Mondays 10-11 AM, Deschutes 362

TA

- Mert Yapucuoglu
- Email: `merty@uoregon.edu`
- Office hours: Wednesdays 1-2 PM and Fridays 3-4 PM, Deschutes 100

Textbooks and Readings

- **Textbook:** *Security in Computing, 6th edition*, by Charles P. Pfleeger, Shari Lawrence Pfleeger and Lizzie Coles-Kemp. ISBN-10: 0137891210.
- **Slides:** Class slides will be provided on Canvas as soon as they are available.

Expected Learning Outcomes

Upon successful completion of the course, students will be able to:

- Understand basic concepts of cryptography, including classic and public key cryptography and use of encryption;
- Understand fundamental concepts and issues with program security, including buffer overflow, computer viruses, and countermeasures against program threats;
- Become familiar with security methods of ordinary operating systems (OS) and concepts and methods for trusted OS;
- Become aware of threats in networks and become familiar with common methods in securing networks and communications, including firewalls and security protocols;
- Understand basic concepts with cloud computing security;
- Grasp essential concepts with security administration, legal and ethical security issues, and privacy; *and*
- Developed experience in working on a term-long class project, including skills ranging from identifying a topic, developing a plan, and executing the plan. CS 433 students will also accumulate team work experience.

Acquired Skills

Upon successful completion of the course, students will have acquired the following essential skills:

- Identifying an interesting security project topic and developing a plan for carrying out the project;
- Exercising a systematic approach to a security problem;
- Improved skills in programming and data analysis; and
- Improved team work and presentation skills.

Estimated Student Workload

The workload of this course is expected to be as follows.

- Class participation. Students should attend the lectures and actively participate in the class, including raising questions and participating discussions.
- Course review and homework.
  - Students should carefully review the class materials after the class.
  - There will be **3-4** homeworks throughout the term. **Late submissions? 10% penalty per day.**

- Class project. **Every** student is required to form a team of 2 or 3 students to work on a class project. With the help of the professor and the TA, every team will identify an interesting problem related to the course material, design, implement, and evaluate a solution, and write a **project report**.

  Warning: The class project can be a lot of fun, but can be also time-demanding. **Start ASAP.**

- Exam.
  - Midterm: **February 22, Thursday**.
  - Final: *No Final Exam.*

Workload expectations are 15-17 hours per week.

Course Requirements and Grading

- Overall:

  Class participation 10% **Homework 15%** **Midterm 35%** **Class Project 40%**

- For class project:

Project proposal 15%	Due: 1/18, 9:59 AM
Project proposal presentation 5%	Slides due: 1/18, 9:59 AM
Midterm report 15%	Due: 2/15, 9:59 AM
Project presentation 10%	Slides due: 3/12, 9:59 AM
Final deliverables 55%	Due: 3/17, 11:59 PM

- Grading rubric:

A+ [95, 100]%	A [90, 95)%	A- [85, 90)%
B+ [80, 85)%	B [75, 80)%	B- [70, 75)%
C+ [65, 70)%	C [60, 65)%	C- [55, 60)%
D+ [50, 55)%	D [45, 50)%	D- [40, 45)%
F [0,40)%		

A Excellent. Solid grasp of concepts, approaches, and/or skills introduced or used in this course. Very well prepared to apply this knowledge to future studies or employment.

B Very good. Generally good grasp of concepts, approaches, and/or skills introduced or used in this course. Prepared to apply this knowledge to future studies or employment.

C Pass. Basic grasp of concepts, approaches, and/or skills introduced or used in this course. Minimally prepared to apply this knowledge to future studies or employment.

D No Pass (Earns UO credit). Demonstrated grasp of concepts, approaches, and/or programming skills introduced or used in this course is not yet sufficient to apply this knowledge to future studies or employment.

F No Pass (No credit). Little or no demonstrated grasp of concepts, approaches, and/or programming skills introduced or used in this course, and/or failure to carry out much of the required work.

A+ Distinction. A+ grades will be given only in cases where the student has excelled in all course topics and overall performance is distinctly better than that required for an A grade.

Schedule(tentative)

Due dates of homework and projects: see the table; due *before* the corresponding lecture begins.

Lecture	*Section*	*Coverage*	*Projects and Homework*
1 (1/9)	1.1–1.7	`syllabus`; introduction	
2 (1/11)	2.1–2.2	`NETSEC research`; authentication and access control	
3 (1/16)		*no class; inclement weather*	
4 (1/18)		`project idea presentation`	
5 (1/23)	2.3	elementary cryptogrphy	project proposal due
6 (1/25)	slides	use of encryption	
7 (1/30)	3.1–3.3	program security	
8 (2/1)	5.1	operating systems security (1)	HW 1 due
9 (2/6)	5.2	operating systems security (2)	
10 (2/8)	6.1–6.3	network security (1)	
11 (2/13)	6.4–6.5	network security (2)	HW 2 due
12 (2/15)	6.6	network security (3)	project midterm report due
13 (2/20)	6.7–6.10	network security (4)	
14 (2/22)	-	`Midterm`	
15 (2/27)	8.1–8.2	cloud security	
16 (2/29)	10.3-4;11.1–8	incidents, risk, legal issues and ethics	HW 3 due
17 (3/5)	9.1–9.7	privacy	
18 (3/7)	13.1–13.4	emerging topics	HW 4 due
19 (3/12)	-	`project presentation`	
20 (3/14)	-	`project presentation`	
			project delivery (report etc.)

Course Policies

Outside Classroom Communication

We encourage everyone to get in touch with the professor when you have a question. Do not postpone your questions until the last couple weeks of the term.

Your email subject should begin with **CS 433:** or **CS 533:** to help email filtering.

Barriers and Accommodations

Our goal is a fully inclusive class, accessible to everyone. If you encounter or anticipate barriers to full participation and fair evaluation for any reason, please communicate your needs to the instructor so that we can find a suitable accommodation. If you encounter or observe other impediments to full participation, for yourself or others, please share your concerns with the instructor. You are also encouraged to contact the Accessible Education Center in 360 Oregon Hall at 541-346-1155 or `uoaec@uoregon.edu`.

It is particularly important that you inform the instructor in the first week of the quarter if you require accommodation. Delayed notification of such a requirement may make it impossible to provide the accommodation.

Academic Honesty

The University Student Conduct Code (available at `conduct.uoregon.edu`) defines academic misconduct. Students are prohibited from committing or attempting to commit any act that constitutes academic misconduct. Students should properly acknowledge and document all sources of information (e.g., quotations, paraphrases, ideas) and use only the sources and resources authorized by the instructor. If there is any question about whether an act constitutes academic misconduct, it is the student's obligation to clarify the question with the instructor before committing to attempting to commit the act.

All projects turned in for the course must be your own work. Copying from other class members or other sources is not acceptable. If you collaborate with someone else on an assignment, you must indicate such on the work you turn in. Collaboration that is not explicitly credited is plagiarism.

Academic honesty is expected and cases of suspected dishonesty will be handled according to university policy. In particular, copying someone else's work (including material found on the web) will not be tolerated. If solutions to assignments are obtained from outside sources, the source must be cited.

You are also responsible for protecting your work. That is, you must take reasonable precautions to prevent your work from being copied. This means that if you store your assignment solutions on a shared server, the file permissions must be set to keep others from accessing your files. If you are working on assignments on a shared machine, you must remove any of your files from the machine before you leave.

Turning in someone else's code is collusion, and is a particularly heinous form of plagiarism; if collusion is detected, all individuals involved (i.e., the copyee and all copyers) will be given a grade of F in the course.

Academic Disruption due to Campus Emergency

In the event of a campus emergency that disrupts academic activities, course requirements, deadlines, and grading percentages are subject to change. Information about changes in this course will be communicated as soon as possible by email and on Canvas. If we are not able to meet face-to-face, students should immediately log onto Canvas and read any announcements and/or access alternative assignments. Students are also encouraged to continue the readings and other assignments as outlined in this syllabus or subsequent versions of the syllabus.

Prohibited Discrimination and Harassment Reporting

Students experiencing any form of prohibited discrimination or harassment, including sex or gender-based violence, may seek information and resources at `safe.uoregon.edu`, `respect.uoregon.edu`, or `investigations.uoregon.edu`, or contact the non-confidential Title IX office/Office of Civil Rights Compliance (541-346-3123), or Dean of Students offices (541-346-3216), or call the 24-7 hotline 541-346-SAFE for help.