

CS 4570-30700 | CS 5070-30860: Network Attack Security
Spring 2025 | January 13, 2025 - May 9, 2025
Department of Computer Science
Oklahoma State University, Stillwater, OK

Course Information:

- Instructor: Dr. Cong Pu, Ph.D.
- Office: 216 MSCS
- Office phone: 405-744-6036
- Email: cong.pu@okstate.edu
- Course format: Traditional classroom course (shown as “Independent Study” in the Banner)
 - Neither lecture will be broadcasted nor recorded.
- Course meetings: Monday/Wednesday, 4:00 pm - 5:15 pm
Stillwater Campus | Classroom Building 217
 - This cross-listed course includes both undergraduate and graduate sections with minor differences regarding course requirements and grading policy.
- Teaching assistant(s):
 - Name / Email: TBA
 - Office hours / Location: TBA / MSCS 203E (SPUR center)
- Office hours (RSI):
 - Tentative office hours: Monday/Wednesday, 3:00 pm - 4:00 pm or by appointment.
 - Students can always meet the instructor during office hours; no appointment is required. Outside office hours, please make an appointment first.
- Course web page (RSI):
 - Canvas <https://canvas.okstate.edu/>. It is important to visit Canvas regularly for up-to-date course information.
 - Lecture slides, source code, virtual machines, and other relevant materials are uploaded to Canvas ***before each class***.
 - If students do not see lecture slides, source code, virtual machines, and other relevant materials on Canvas before the class, please send an email to remind the instructor.

Course Description:

- This advanced course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks.
- After completing this course, students will familiarize themselves with the latest developments in cybersecurity, including practical guides to design, implementation, and testing industrial networks and applications to ensure their security and reliability in an industrial production environment.

Prerequisites:

- CS 3443: Computer Systems; CS 4243: Intro to Computer Security; CS 4283: Computer Networks

Course Objectives (CO): Students who have completed this course should have:

| Course Objective | How students will practice each outcome in this course | How student achievement of each outcome will be assessed in this course |
|---|--|---|
| CO-1: Design, develop and implement a secure Cyber-infrastructure and Security Operation Center. | Lecture Examples In-class exercise/discussion | Assignments Capture the Flag (CTF) Exams |
| CO-2: Assess network defenses and computer system's security vulnerabilities and detect attempted security breaches using appropriate tools and resources. | Lecture Examples In-class exercise/discussion | Assignments Capture the Flag (CTF) Exams |
| CO-3: Utilize security technologies such as firewalls, VPNs, virtualization, virus scanning, intrusion protection and patches to industrially harden a cyber-infrastructure. | Lecture Examples In-class exercise/discussion | Assignments Capture the Flags (CTF) Exams |

Preferred Communication Method and Expected Response Time (RSI):

- Students can always meet with the instructor during office hours, no appointment is required.
- Outside office hours, please send an email to the instructor to make an appointment first.
- When students send an email to the instructor, please use OSU email account, and include a course number, e.g., CS 4570 or CS 5070, in the subject line.
- Students can generally expect an email response within 6 hours. If students do not get a response within 6 hours, please forward the previous email to the instructor.
- Students can generally expect feedback on review quizzes, assignments, capture the flags, and exams in two weeks after submission. If students do not receive feedback in three weeks, please send an email to the instructor.

Required Textbooks, Additional Reading, and Other Materials:

- Computer & Internet Security: A Hands-on Approach. Wenliang Du. 3rd Edition. ISBN-13: 978-1733003940. ISBN-10: 1733003940.
- Important concepts/materials will be included in the lecture notes from various sources and uploaded to Canvas.

Course Requirements and Grading Policy:

- **1st Exam [10%]:** February 10 (Monday), 4:00 pm - 5:15 pm, Stillwater Campus | Classroom Building 217
- **2nd Exam [10%]:** March 26 (Wednesday), 4:00 pm - 5:15 pm, Stillwater Campus | Classroom Building 217
- **3rd Exam [10%]:** May 5 (Monday), 6:00 pm – 7:50 pm, Stillwater Campus | Classroom Building 217
 - All exams are non-cumulative, open notes and paper-based.
 - All exams should be taken in the classroom (Stillwater Campus | Classroom Building 217). However, students can start the exam whenever they want during the exam time. The exam paper should be submitted by the end of exam time.
 - Students are allowed to bring notes on one piece of double-sided A4 paper.
 - Other resources and the Internet are NOT allowed.

- Students can write/print/draw any notes on the double-sided A4 paper.
- There will be NO make-up for missing exam. Only university excused absences with appropriate and official **DOCUMENTATION** will be accepted for the make-up exam.
 - The make-up exam must be taken within three days after the scheduled exam.
- If students take a conflict exam, they must inform the instructor and provide a valid **DOCUMENTATION** at least two weeks before the scheduled exam.
 - The conflict will be resolved based on Oklahoma State University Policy and Procedures – POLICY 1.01 <https://adminfinance.okstate.edu/site-files/documents/policies/final-exam-overload-and-common-final-or-evening-exam-conflict.pdf>.
 - The conflict exam must be taken within three days after the scheduled exam.
- **1st Capture the Flag (CTF): CS 4570-30700 [7.5%] | CS 5070-30860 [10%]:**
 March 5 (Wednesday), 4:00 pm - 5:15 pm, Stillwater Campus | Classroom Building 217
- **2nd Capture the Flag (CTF): CS 4570-30700 [7.5%] | CS 5070-30860 [10%]:**
 April 21 (Monday), 4:00 pm - 5:15 pm, Stillwater Campus | Classroom Building 217
 - All CTFs are **comprehensive, open resources** and **computer-based**.
 - All CTFs should be completed in the classroom (Stillwater Campus | Classroom Building 217). However, students can start the CTF whenever they want during the scheduled time. The CTF should be submitted by the end of scheduled time.
 - There will be NO make-up for missing CTF. Only university excused absences with appropriate and official **DOCUMENTATION** will be accepted for the make-up CTF.
 - The make-up CTF must be taken within three days after the scheduled CTF.
 - If the student has a time conflict between the CTF and the activities from other classes, they must inform the instructor and provide a valid **DOCUMENTATION** at least two weeks before the scheduled CTF.
 - The conflict will be resolved based on Oklahoma State University Policy and Procedures – POLICY 1.01.
 - The conflict CTF must be taken within three days after the scheduled CTF.
- **Assignment: CS 4570-30700 [55%] | CS 5070-30860 [50%]:**
 - Assignment should be submitted on **Canvas** <https://canvas.okstate.edu/>. Other submission methods (i.e., email) will **NOT** be accepted.
 - **LATE** submission will **NOT** be accepted on Canvas <https://canvas.okstate.edu/> since the submission link will be closed automatically after due date.
 - The deadline is **ALWAYS 4:00 pm** (not 11:59 pm or midnight) on the due date.
 - 1 minute late and 1 hour late are treated the same: late submission.
 - There will be NO re-submission for missing assignment. Only university excused absences with appropriate and official **DOCUMENTATION (covering half of assignment time)** will be accepted for assignment re-submission.
 - Each student has **unlimited** submission attempts on Canvas <https://canvas.okstate.edu/> **before due date**. However, the TA only grades the last submission attempt.
 - There will be NO re-submission if the student submitted the **WRONG** assignment. So, please **VERIFY** the uploaded assignment after the submission.
 - Students need to refer to detailed **submission guidelines** in the assignment when they intend to submit the assignment on Canvas.
 - E.g., when asked to upload source codes, students should upload the actual source code rather than providing a link to the codes on the cloud.
- **Review Quiz [5%] (Bonus):**

- Review quiz will **NOT** be announced in advance, so attendance is highly **REQUIRED**.
- There will be NO make-up for missing review quiz due to absence, lateness, etc.. Only university excused absences with appropriate and official **DOCUMENTATION** will be accepted for the make-up review quiz.
- Plagiarism:
 - Plagiarism or cheating will not be tolerated in the class.
 - 1st plagiarism will result in zero point in the suspected work.
 - 2nd plagiarism will result in immediate dismissal (F grade).
 - **AI Usage Statement:** Students may access and use generative AI tools, such as ChatGPT, Bing AI, or Bard, to assist them in their learning of the course content. Appropriate uses may include generating ideas for writing assignments, checking facts of a phenomenon, and assessing a paper for grammatical errors that are written by the student. Such uses of the tool assist students in learning the content and will therefore be permitted. However, students are prohibited from using generative AI tools to completely produce, reproduce, and/or manufacture paper and/or other assignments without using any personal effort devoted to the learning process. Before using generative AI tools, students should check to ensure they do not conflict with copyright laws or other's proprietary information.
- All grades will be posted on Canvas <https://canvas.okstate.edu/>:
 - *Students are highly suggested to check the grade on Canvas <https://canvas.okstate.edu/> frequently and notify instructor immediately if there is any grading error.*
 - Students are required to communicate with the TA for any grading error.
 - Mid-term grade will be posted by Friday, April 11, 2024.
 - **Friday, April 11, 2024:** last day to drop an individual course.
- Grade Scale:
 - Actual points received in each category should be converted into category percentage. For example, if you got 40 for 5 assignments (10 pts for each assignment), the percentage of assignment category will be $(40 / 50) * 55\% = 44\%$.
 - A (100 - 90), B (89 - 80), C (79 - 70), D (69 - 60), and F (59 - 0)
- **Excuses:**
 - Because there is a degree of flexibility in completing items, it is the student's responsibility to keep track of important dates/announcements (e.g., class and email announcements) and find enough time for completion. If students procrastinate and wait until the last minute to complete or submit their work, there is no one to blame but the students themselves if unexpected/ unanticipated/undesired things happen. With that said, the instructor is also not heartless. *If there is something that occurs which prevents student's access to the course for a significant length of time (e.g., serious illness, death in the family, or personal tragedy), the student needs to contact the instructor as soon as possible with appropriate and official DOCUMENTATION and they may be able to work something out.* If the student chooses to wait until the end of semester to contact the instructor for excuses and accommodation, there is nothing the instructor can do.

Attendance Policy:

- The instructor chooses **NOT** to take attendance. However, students are expected to attend all class meetings punctually to receive the bonus points of review quizzes, from the beginning until the end of the semester.

- The student does not have to inform the instructor if s/he has to miss class(es).
- If the student misses class(es) due to a university-excused absence, s/he should contact the instructor and provide the necessary official **DOCUMENTATION** for the make-up work.
- If a student misses a class without university excused absence documentation, the student should not expect individualized instruction on what was missed. This will be effective from the beginning of the semester.

Civility in the Classroom Statement:

- Oklahoma State University is a community of faculty, students, and staff that enjoys an expectation of cooperation, professionalism, and civility during the conduct of all forms of university business, including the conduct of student–student and student–faculty interactions in and out of the classroom. Further, the classroom is a setting in which an exchange of ideas and creative thinking should be encouraged and where intellectual growth and development are fostered. Students who disrupt this classroom mission by rude, sarcastic, threatening, abusive or obscene language and/or behavior will be subject to appropriate sanctions according to university policy. Likewise, faculty members are expected to maintain the highest standards of professionalism in all interactions with all constituents of the university.
 - To ensure that you are fully engaged in class discussions during class time, you are expected to do the following:
 - Maintain the level of civility and professionalism expected in a face-to-face classroom setting.
 - Refrain from engaging in non-class related activities during class time that creates a distraction for other students in the class and/or limit your ability to engage in the course.
- Failure to meet these expectations may result in the following consequences:
 - Being counted as absent for the class meeting.
 - Not receiving credit for class participation for that class period.
 - Other consequences as stipulated in the syllabus, Oklahoma State University The Student Code of Conduct, or other university policy.

Student with Disabilities:

- Any student who is registered with Student Accessibility Services (SAS) office and may require special arrangements/accommodations in order to meet the course requirements should contact the instructor as soon as possible to make any necessary arrangements/accommodations. Students should present appropriate verification from Student Accessibility Services <https://accessibility.okstate.edu/> during the instructor's office hours. Please note instructors are not allowed to provide classroom accommodations to a student until appropriate verification from Student Accessibility Services has been provided. For additional information, you may contact the Student Accessibility Services office in 155 UHS or 405-744-7116 / accessibility@okstate.edu.

Academic Integrity Statement:

- Oklahoma State University is committed to the maintenance of the highest standards of integrity and ethical conduct of its members. This level of ethical behavior and integrity will be maintained in this course. Participating in a behavior that violates academic integrity (e.g., unauthorized collaboration, plagiarism, multiple submissions, cheating on

examinations, fabricating information, helping another person cheat, unauthorized advance access to examinations, altering or destroying the work of others, and fraudulently altering academic records) will result in your being sanctioned. Violations may subject you to disciplinary action including the following: receiving a failing grade on an assignment, examination or course, receiving a notation of a violation of academic integrity on your transcript, and being suspended or dismissed from the University. Oklahoma State University's Academic Integrity policy identifies behaviors that violate the fundamental values of academic integrity. Please refer to <https://academicaffairs.okstate.edu/academic-integrity/academic-integrity.html> for more information.

Discrimination, Harassment, and Sexual Violence Statement:

- Oklahoma State University is committed to providing and strengthening an educational, working, and living environment where students, faculty, staff, and visitors are free from gender and/or sex discrimination of any kind. Sexual assault, discrimination, harassment, and other Title IX violations are not tolerated by the University. Report any incidents to the Office of Equal Opportunity Services, 405.744.1156 or file a report online at <https://hr.okstate.edu/equal-opportunity/title-ix-process.html>.

Additional Information:

- The instructor views the syllabus as a **contractual agreement** between the instructor and students, which means the instructor will **completely follow** the syllabus while advising, teaching, testing, and evaluating students in this course.
 - **If there are any differences between what the instructor says inside or outside the classroom and the information on the syllabus, please refer to the syllabus as the standard.**
 - By enrolling in the class, the student agrees to **fully adhere** to the syllabus throughout s/he studies.
 - The instructor reserves the right to **propose changes** to the syllabus as deemed necessary / with reasonable reasons.
 - Any changes will be announced in the classroom as early as possible and will be implemented if the majority of attending students approve them via **voting**.
- The syllabus lets students know what the course is about, why the course is taught, where it is going, and what will be required for them to be successful in the course.

Technology/Skills Requirements:

- To be enrolled in this course, students **MUST READ, AGREE TO, and SIGN** the **Cybersecurity Ethics Agreement** during the first class.
- The instructor firmly believes in **'learning by doing' for cybersecurity**. Therefore, this course includes **a significant number of hands-on activities**. If you are **uncomfortable with hands-on activities**, please **consider withdrawing** from the course.
- Students **NEED** to possess a **personal computer** for hands-on activities.
- Students **MUST** be proficient in, or willing to learn, the use of Linux-based OS, programming languages (C, C++, and/or Python), computers, the Internet, web browsers, Microsoft Office, PDF readers, Virtual Machine (VM) players, code editors, and other common computer applications.

Course Schedule and Important Dates: Topics and/or dates may be changed during the semester at the instructor's discretion because of scheduling issues, developments in the discipline, or other contingencies. If there is any change, students will be notified immediately.

- January 13: Syllabus | Course Introduction | Q&A
- January 15: Packet Sniffing and Spoofing
- **January 20: University Holiday (No Class)**
- January 22: Packet Sniffing and Spoofing
- January 27: Packet Sniffing and Spoofing
 - Release Assignment 1
- January 29: TCP Protocol and Its Attacks
- February 3: TCP Protocol and Its Attacks
- February 5: TCP Protocol and Its Attacks
 - Assignment 1 Due | Release Assignment 2
- **February 10: 1st Exam**
- February 12: Buffer Overflow Attack
- February 17: Buffer Overflow Attack
- February 19: Buffer Overflow Attack
 - Assignment 2 Due | Release Assignment 3
- February 24: Penetration Testing
- February 26: Penetration Testing
- March 3: Penetration Testing
 - Assignment 3 Due | Release Assignment 4
- **March 5: 1st Capture the Flag (CTF)**
- March 10: Firewalls
- March 12: Firewalls
- **March 17: Students' Spring Break (No Class)**
- **March 19: Students' Spring Break (No Class)**
- March 24: Firewalls
 - Assignment 4 Due | Release Assignment 5
- **March 26: 2nd Exam**
- March 31: Race Condition Vulnerabilities
- April 2: Race Condition Vulnerabilities
- April 7: Race Condition Vulnerabilities
 - Assignment 5 Due | Release Assignment 6
- April 9: Format String Vulnerability
- April 14: Format String Vulnerability
- April 16: Format String Vulnerability
 - Assignment 6 Due | Release Assignment 7
- **April 21: 2nd Capture the Flag (CTF)**
- April 23: Web Security
- April 28: Web Security
- April 30: Web Security
 - Assignment 7 Due
- **May 5: 3rd Exam, 6:00 p.m. – 7:50 p.m.**