CEG 4420/6420 – Host Computer Security

Fall 2025

Instructor: Darron Johnson (Darron.Johnson@wright.edu)

Department of Computer Science & Engineering

Wright State University

E-mail: Darron.Johnson@wright.edu
Credits: 3

Course Description:

This course delves into the fundamental principles in computer security, including software security and hardware security. The goal is to help students understand programs and their running environments (software and hardware), the corresponding vulnerabilities and their consequences, different conditions and techniques to exploit vulnerabilities for initiating attacks, and specific countermeasures to defend against these attacks.

Learning Outcomes:

Students who successfully complete this course will be able to:

- Acquire in-depth knowledge on different software and hardware vulnerabilities (causes and consequences) and attacks built on these vulnerabilities (detailed implementations)
- Explore different mitigation strategies to address software and hardware security issues
- Gain hands-on experience in assessing attacks and implementing defenses
- Apply static code analysis tools
- Demonstrate existing malware, and distinguish detection, prevention, mitigation and repair
- Improve security and privacy by proper configuration, fortification, and hardening of operating systems.

Required Course Materials:

(Week 1-13) Textbook #1:

Charles Pfleeger, Shari Lawrence Pfleeger, Lizzie Coles-Kemp, *Security in Computing, 6th Edition.* Pearson Education, 2024.
ISBN-13: 978-0-13-789121-4
ISBN-10: 0-13-789121-0

(Week 14-16) Textbook #2:
Swarup Bhunia, Mark M. Tehranipoor, *Hardware Security – A Hands-on Learning Approach, 1ST Edition.* Elsevier, 2019.
ISBN: 978-0-12-812477-2

Methods of Instruction

This class session will be offered in an asynchronous online modality.

Asynchronous: Students will review the weekly lectures and assignments provided in each module at their earliest convenience (within the assigned dates of the module). Discussion questions will also be in additional component to promote interpersonal engagement with your classmates.

Course Communications & Administration

- **Webex** will be used for all office hour appointments or one-on-one sessions with Professor Johnson.
- **Emails** will be responded to within 24 hours.
- **News** - a section of the course webpage on Pilot where important course information will be posted.

Course Policies

- Homework and projects should be submitted by the corresponding due date and time.
- Late work will be penalized at 20% of its full credit for every 24 hours it is late.
- All written assignments will be developed using the standard APA format, to include: MS word, 12-point Times New Roman font, 1.5 line spacing and 1-inch margins. This format is required for all written papers.
- Please use the following link for all references for APA formatting: https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_style_introduction.html
- Unless specifically directed by the instructor, using Generative AI tools to accomplish or help accomplish course assignments is strictly prohibited.

Reasonable Accommodations: Any student with a disability or other special need is encouraged to:

- Share these concerns or requests with the instructor as soon as possible
- Pursue assistance from the university Office of Disability Services (https://www.wright.edu/disability-services)

Academic Integrity and Ethical Learning

• Students must adhere to the "Academic Integrity" of the Code of Student Conduct at Wright State University (https://policy.wright.edu/policy/3710-academic-integrity-standards-and-process-misconduct)

• The knowledge gained in this course must be applied responsibly and never used for unethical or harmful purposes.

• **Generative AI Tools:** The use of AI tools to complete assignments or portions of assignments is not permitted unless explicitly allowed by the instructor. For any assignments where AI tool use is authorized, you must clearly disclose which tools were used, how they were used, and which parts of the assignment were created with AI assistance. If you're unsure whether a specific tool or technology is allowed, consult your instructor before using it. Keep in mind that all submitted work will be graded according to the assignment's criteria, regardless of how it was created. AI-generated content may not meet the required standards for accuracy or quality, and using such tools does not guarantee a passing grade. You are responsible for reviewing and verifying any AI-generated material to ensure it meets expectations. Ultimately, your grade will reflect the quality of the work you submit.

Graduate Student Assignments: Graduate students enrolled in CEG 6422 are expected to complete 50% more coursework than undergraduate students over the duration of the semester. This additional work will include research papers, class presentations, additional exam questions, and other activities centered around topics in secure computing.

Learning Assessments: Student learning and assessment will take place through a combination of weekly exercises, quizzes, discussion forums, and exams. Quizzes, homework assignments, and exams are to be completed independently and must reflect each student's own work—collaboration on these is not permitted. In contrast, weekly exercises and discussion forums include both individual and collaborative components. Students are strongly encouraged to engage with their peers and collaborate where appropriate to enhance learning and enrich discussion.

Quizzes: Quizzes will consist of 15-20 questions about assigned reading material, videos and lecture content.

Discussion Forum Assignments: Each week, students are expected to actively participate in the course discussion forum by responding to the assigned topic. An initial post is required by Wednesday at midnight (11:59 PM) and should demonstrate a clear understanding of the material, thoughtful analysis, and meaningful reflection. In addition to the initial post, students must respond to at least two peers by Sunday at midnight (11:59 PM). These peer responses should go beyond simple one-liners or basic agreement; instead, they should engage in meaningful dialogue by asking questions, offering different perspectives, elaborating on ideas, or connecting the discussion to course content or real-world examples. While consistent participation is important, quality should be prioritized over quantity. Posts should reflect respectful, constructive engagement and contribute to a deeper exploration of the topic. Students are also encouraged to monitor and reply to responses on their own posts to keep the conversation going and foster a collaborative learning environment.

All exams will be administered during Week 8 and Week 16, aligned with the respective modules, and must be submitted by midnight on the final day of each module (Sunday).

Grading Scale and Breakdown:

A = 90-100
B = 80-89
C = 70-79
D = 60-69
F = 59 and below

CEG 4420 Undergraduate Students
Weekly Assignments: 20%
Discussion Forums: 20%
Quizzes: 20%
Lab Exercises: 20%
Midterm Exam: 30%
Final Exam 30%

***CEG 6420 Graduate Students**
Weekly Assignments: 20%
Discussion Forums: 20%
Quizzes: 20%
Lab Exercises: 20%
Midterm Exam: 30%
Final Exam: 30%
Research Paper/Presentation: 30%

Undergraduate students and graduate students will be graded separately

WEEKLY COURSE OUTLINE

Week	Topics	Chapter Readings	Activities and Testing
1	**Textbook #1: Security in Computing** **Introduction**	Chapter 1	Please see weekly assignment breakdown within the course shell.
2	**Identifying Tactics of Advanced Persistent: Threats with Limited Attack Traces**	University System Publication	Please see weekly assignment breakdown within the course shell.
3	**Textbook #1: Security in Computing** **Programs and Programming**	Chapter 3	Please see weekly assignment breakdown within the course shell.
4	***Textbook #2: Hardware Security*** **Side-Channel Attacks**	Chapter 8	Please see weekly assignment breakdown within the course shell.
5	**Textbook #1: Security in Computing** **Operating Systems**	Chapter 5	Please see weekly assignment breakdown within the course shell.
6	***Textbook #2: Hardware Security*** **Test-Oriented Attacks**	Chapter 9	Please see weekly assignment breakdown within the course shell.
7	**Textbook #1: Security in Computing** **Data and Databases**	Chapter 7	Please see weekly assignment breakdown within the course shell.
8	**Textbook #1: Security in Computing** **New Territory**	Chapter 8	Midterm exam week
9	***Textbook #2: Hardware Security*** **Physical Attacks and Countermeasures**	Chapter 10	Please see weekly assignment breakdown within the course shell.
10	**Textbook #1: Security in Computing** **Management and Incidents**	Chapter 10	Please see weekly assignment breakdown within the course shell.

11	**Textbook #1: Security in Computing** **Legal Issues and Ethics**	Chapter 11	Please see weekly assignment breakdown within the course shell.
12	***Textbook #2: Hardware Security*** **Security, Threat Assessment, and Design for Security**	Chapter 13	Please see weekly assignment breakdown within the course shell.
13	**Textbook #1: Security in Computing** **Emerging Topics**	Chapter 13	Please see weekly assignment breakdown within the course shell.
14	***Textbook #2: Hardware Security*** **Hardware Trojans**	Chapter 5	Please see weekly assignment breakdown within the course shell.
15	***Textbook #2: Hardware Security*** **Attacks on PCB: Security Challenges and Vulnerabilities**	Chapter 11	Please see weekly assignment breakdown within the course shell.
16	***Textbook #2: Hardware Security*** **System Level Attacks and Countermeasures**	Chapter 16	Final exam

Note: This course outline is subject to change.