CPTS/EE 439: Cybersecurity of Critical Infrastructure Systems

Course Syllabus — Spring 2024

Course Credits: 3
Meeting time: Monday, Wednesday, Friday, 1:10-2:00 PM (Jan 08-Apr 26)
Classroom: Sloan 7
Course webpage: https://wsucpts.gitbook.io/cpts439sp24/

Instructor: Monowar Hasan
Office location: EME B53
Email: monowar.hasan@wsu.edu
Phone: +509 335 8352
Office hours: Monday, Wednesday, 2:30-3:30 PM, or by appointments

Class announcements: Canvas
Homework/lab submissions and grades: Canvas and GitHub Classroom

How to Use this Syllabus

This syllabus provides you with course-specific information and important university policies. This document should be viewed as a course overview; it is not a contract and is subject to change as the semester evolves. Changes to the syllabus will be announced on Canvas.

---

1 Course Overview

This course aims to systematically understand critical cyber-physical systems (CPS) and covers the principles, techniques, and challenges of securing such systems. Students will gain a deep understanding of the vulnerabilities and threats in these systems and learn how to design and implement security measures. Example domains that we will study include the security of industrial control systems, automotive systems, smart grids, time-critical systems, and commodity Internet-of-things (IoT). Topics covered include secure communication protocols, system-level defense, intrusion detection systems, risk assessment, and incident response.

Students completing this class will be able to:

1. Demonstrate the ability to discover and understand the cyber-physical environment and identify the challenges to protect them.
2. Classify existing vulnerabilities of critical systems and categorize defense strategies.
3. Design security solutions to protect critical cyber infrastructures.

Catalog Description. Course Prerequisite: CPTS 327 and 426 with a C or better or concurrent enrollment; admitted major or minor in EECS or Data Analytics; OR EE 234 and 361; admitted major or minor in EE; OR CPTS 327 and E E 234; admitted major or minor in Cpt Engr. Security topics as they relate to critical infrastructure systems vital to any nation including industrial control systems, cyber physical systems, SCADA, DCS, IoT, IIoT, and the knowledge to secure such systems. (Crosslisted course offered as EE 439, CPTS 439). Typically offered in Spring.

2 Learning Objectives

This class contributes to the following ABET Student Outcomes (SOs):

- **SO 1:** Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.
- **SO 2:** Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- **SO 3:** Communicate effectively in a variety of professional contexts.
- **SO 6:** Apply computer science theory and software development fundamentals to produce computing-based solutions.
- **SO 7:** Acquire and apply new knowledge as needed, using appropriate learning strategies.

Note: The CS ABET Accreditation is detailed here:
https://vcea.wsu.edu/undergraduatestudies/abet-accreditation/computer-science-bs-pullman/.

3 Prerequisites

Official prerequisites for this course are the following.

- CPTS 327 and 426 with a C or better or concurrent enrollment; admitted major or minor in EECS or Data Analytics; OR
- EE 234 and 361; admitted major or minor in EE; OR
- CPTS 327 and EE 234; admitted major or minor in CE.

Development Background. The class will involve programming in C/C++ and Python. Students should also have experience with command line interfaces, version-controlling systems (Git), and programming in a Linux environment.

4 Textbook

The course uses materials from state-of-the-art cyber-physical and IoT security literature. In-class discussions and lecture slides will be sufficient to understand the basic concepts. No textbook is required.

Optional Reading

Safety and Security of Cyber-Physical Systems, Frank J. Furrer
DOI: https://doi.org/10.1007/978-3-658-37182-1
Available through WSU Libraries: https://link.springer.com/book/10.1007/978-3-658-37182-1

5 Content Outline and Schedule

The tentative weekly schedule is given below. This schedule may be revised as the course progresses. The updated schedule and class lectures will be available on the course website.

Week	Topics
Week 1	Course logistics and overview, CPS background
Week 2	CPS security primitives
Week 3	Industrial network design
Week 4	Industrial network protocols
Week 5	Attacking industrial networks
Week 6	Isolation techniques
Week 7	Mid-term review Mid-term exam (Friday)
Week 8	Automotive system security
Week 9	Access control
Week 10	Anomaly and threat detection
Week 11	No class (Spring vacation)
Week 12	Securing smart-grid
Week 13	Real-time security
Week 14	Hardware security
Week 15	Security auditing
Week 16	Buffer days, recap, and closing
Week 17	Final exam

6 Reading Assignments

Three reading assignments will be released on Week 2, Week 10, and Week 13. These exercises may encompass conceptual questions as well as small programming challenges. Grading for these assignments will be based on *submission* or *non-submission*: total points for attempted assignments with reasonable answers will be awarded; unattempted tasks will receive no points. The reading assignments will be beneficial for comprehending concepts and preparing for exams.

7 Programming Assignments

There will be four programming assignments. The following is the tentative schedule for the assignments.

Release	Deadline	Assignment
Week 3	Week 4	Security analysis of an embedded firmware image
Week 5	Week 6	Attacking a cyber-physical plant
Week 8	Week 9	Hacking an automotive system
Week 10	Week 12	UAV autopilot controller security

We will use GitHub Classroom to deliver the assignments. Detailed instructions for assignment submission will be provided on the course website. If you have not used GitHub before, we recommend creating a GitHub account by Week 3.

8 Term Project

Students will engage in a semester-long project related to critical infrastructure security. A team of a maximum of two students is acceptable. The students will submit an end-of-semester report and a recorded presentation (time limit: 10 minutes).

The term project could be one of the following types:

1. **Survey:** Students will survey the related research fields. The survey should summarize at least 8 papers from top journals/conferences.
2. **Exploration:** Students will explore a new research problem related to CPS/IoT security.

Additional details will be discussed in the class.

8.1 Project Deliverable

- **Project proposal.** The term project proposal with a timeline (max two pages) must be submitted and approved by the instructor by the end of Week 4.
- **Mid-semester update.** A progress report (max three pages) of the project is due by Week 10.
- **Final submission.** The final project submission includes a report, all related code/data, and a recorded talk (maximum 10 minutes). Use the IEEE conference format template for your report (available here: https://www.ieee.org/conferences/publishing/templates.html). Reports can be up to 6 pages, excluding references (and appendices, if any). The final project is due by Week 15.

9 Exam Information

The course will consist of two exams.

Week	Exam
Week 7	Mid-Term Exam (45 minutes) *Includes lecture materials from Week 1-Week 7*
Week 17	Final Exam (1 hour 30 minutes) *Topics include all lecture materials and programming assignments*

All exams are closed-book and must be attempted by all students. Students can bring a handwritten cheat sheet (maximum one page, US letter size). Further details will be discussed before the exam. Unless otherwise specified, the first two exams will take place during the lecture hours programmed for this course. All exams will take place in-person.

Final Exam Information. Final exams are scheduled for the last week of the semester; the Final Exam Schedule is posted on the Registrar's website (www.registrar.wsu.edu).

10 Communication

We will communicate announcements through Canvas and Microsoft Teams. Lecture materials and other learning resources will be accessible on Teams and the course website. Off-class Q&A sessions will be conducted via Teams channels. To streamline communication, if you have questions about course materials, lectures, or project milestones, please post them on the Teams channels instead of emailing them. We

recommend enabling notifications on Teams channels to stay updated on important course logistics and extended lecture discussions initiated by fellow students' questions.

Canvas will serve as the platform for submitting homework assignments and for grading. The programming labs will be managed using a combination of GitHub Classroom and Canvas.

11 Class Participation

Students should make all reasonable efforts to attend all class meetings. While additional slides will be available online, using these materials and textbooks aims to enhance preparedness for in-class sessions, yet they cannot replace the value of attending lectures. Consequently, the course expects students to attend every class, engaging actively and constructively in discussions. Class participation will be assessed based on contributions to in-class discourse, discussions, and questions. Frequently missing class meetings may increase difficulty in understanding exam materials and assignments.

12 Late Submission Policy

Late homework or programming assignments **will not be accepted** unless accompanied by a strong and documented reason, such as medical or family emergencies. Without a valid reason, late submissions will not be graded.

Missed exams with a compelling and documented reason **may be accommodated** and will receive a grade at the instructor's discretion.

13 Grading Policy

The final course grade will be calculated using the following breakdown:

- Class participation 05%
- Reading Assignments 15%
- Programming Assignments 20% (5% each)
- Term Project 30%
- Mid-Term Exam 15%
- Final Exam 15%

We will convert the numeric scores to letter grades using the following scale mapping:

Score	Grade	Score	Grade	Score	Grade
≥ 90	A	[70, 75)	B-	[50, 55)	D+
[85, 90)	A-	[65, 70)	C+	[45, 50)	D
[80, 85)	B+	[60, 65)	C	< 45	F
[75, 80)	B	[55, 60)	C-		

Incomplete Grades. Academic Regulation 90 (https://registrar.wsu.edu/academic-regulations/) states that a grade of Incomplete (I) may be entered only if "the student is unable to complete their work on time due to circumstances beyond their control." Incomplete grades will be handled on a case-by-case basis at the discretion of the instructor.

14 Expectations for Student Effort

Beyond the time for lecture attendance, students are expected to invest a minimum of 4 hours outside class for each lecture equivalent (or 8 hours per week), including the time for working on homework and programming assignments.

15 Academic Integrity

Academic integrity is the cornerstone of higher education. Therefore, all university community members share the responsibility of upholding and promoting the principles of integrity in all activities, including academic pursuits and honest scholarship. Academic integrity will be rigorously enforced in this course.

The students are responsible for reading WSU's Academic Integrity Policy (https://communitystandards.wsu.edu/policies-and-reporting/academic-integrity-policy/), which is based on Washington State law (https://apps.leg.wa.gov/wac/default.aspx?cite=504-26-202).

If you cheat in your work in this class, you will:

1. Receive a **-100% (i.e., Zero)** for that work (homework, lab, exam). The second offense will result in an **automatic F** grade.
2. Be reported to the Center for Community Standards (https://communitystandards.wsu.edu/).
3. Have the right to appeal the instructor's decision.
4. Not being able to drop the course or withdraw from the course until the appeals process is finished.

It will be at the discretion of the grader (if applicable) and the instructor to determine if any assignment displays evidence of collaboration exceeding these boundaries. Any effort to evade the intent of these regulations will be regarded as a breach of the essential directive. Avoid providing or seeking assistance from fellow students. Please consult the instructor if you have inquiries about permissible actions in this course.

If you want to ask for a change in the instructor's decision about academic integrity, use the following form: https://cm.maxient.com/reportingform.php?WashingtonStateUniv&layout_id=10, available at the Center for Community Standards website (https://communitystandards.wsu.edu/). You must submit this request within 21 calendar days of the decision.

What is allowed?

- Engaging in discussions with classmates, TAs, or the instructor about potential approaches or strategies for solving homework problems or completing lab assignments is allowed.
- All homework and labs should be completed individually, including the writing of reports.

What is not allowed (and would be considered as dishonesty/plagiarism/cheating)?

- Copying (verbatim or with slight modifications) homework, code, lab reports, or any other course-related submissions from other students or online sources is prohibited.
- Disseminating or sharing one's own homework solutions, code, or other course submission material with others is prohibited. Please take measures to protect your submissions and code, both physically and digitally. You will be held responsible even if your homework or lab code is copied without your consent.

- Referring to online or Internet sources, AI tools, or textbook solution guides for completing homework or programming assignments is permissible. If you incorporate code obtained from online sources or AI tools into your lab work, providing clear citations or acknowledgments of the original author or tool is required. When presenting AI-generated outcomes, include the specific prompt(s) that led to the solution. Besides, the corresponding section of the assignment should be marked with the following statement: ***"This part of this assignment is completed using AI tool <name>."*** However, utilizing external resources may lead to potential grading penalties; it is advisable to consult the instructor before utilizing such sources.
- Using unauthorized means to complete homework, exams, or labs is prohibited.
  Remember: If in doubt, please check with the instructor!

16 University Policy

Students are responsible for reading and understanding all university-wide policies and resources about all courses (for instance, accommodations, care resources, policies on discrimination or harassment), which can be found in the university syllabus (https://syllabus.wsu.edu/university-syllabus/).