Course Syllabus

Course Information

Course Prefix, Number, Section: CS 6301.002
Course Title: Special Topics in Computer Science - Cyber-Physical System Security
Term: Fall 2026
Modality: Traditional
Times: MW 10-11:15am
Location: ECSW 1.365

Professor Contact Information

Instructor: Chung Hwan Kim

Office Phone: 972-883-3551

Office Location: ECSS 3.201

Email Address: chungkim ‘at’ utdallas ‘dot’ edu

Office Hours: Mon 11:30am-12:30pm (this could be changed at the instructor’s discretion)

Course Website: https://crs.s3lab.io/cs6301/2026/fall/

Course Modality and Expectations

Instructional Mode	Traditional
Course Platform	The course will be taught face-to-face. Instructor and students meet according to the schedule. Limited availability due to classroom spacing.
Expectations	After completing the course, students are expected to gain the abilities to: (1) understand and explain fundamental security concepts, (2) understand common threats and recognize vulnerabilities of information systems, (3) understand and apply cryptographic algorithms, and (4) understand and apply security policies.
Asynchronous Learning Guidelines	Students are mandated to attend class synchronously. Students *should* consult the instructions *in advance* and get excuses, in case they cannot attend the class on time for any reason.

Course Pre-requisites, Co-requisites, and/or Other Restrictions

Students are required to satisfy the following prerequisites:

- Algorithm Analysis and Data Structures (CS 5343)
- Operating System Concepts (CS 5348)

Course project would require students with the following skills:

- Familiarity with command line Unix/Linux
- Understanding and debugging a C/C++ program (e.g., using GDB)
- Basic understanding on how a program executes at low machine instructions and operating systems levels (e.g., basic level of IA-32 assemblies, how a process is created, and how system calls are handled)

Course Description

A comprehensive study of the principles and practices of cyber-physical systems (CPS) security, covering hardware platforms, software systems, and a range of attacks and defenses. Topics include CPS hardware organization (microcontrollers, industrial control systems, robotic and autonomous vehicles, sensors, and actuators); CPS software (communication protocols, real-time requirements, control algorithms, sensor filtering, autonomy frameworks, and simulators); and security challenges and countermeasures across domains, such as sensor spoofing and jamming, network and software vulnerabilities, system-level exploits, and adversarial machine learning attacks.

Student Learning Objectives/Outcomes

Students shall be able to understand the hardware and software foundations of cyber-physical systems, the unique threats and vulnerabilities they face, and the principles and techniques for securing them. They will learn to analyze CPS from an adversarial perspective, study practical attacks on sensors, networks, control software, and AI components, and evaluate corresponding defenses. Students will also be able to assess the significance of CPS-specific threats, reason about real-time and safety-critical constraints, and gauge the protections and limitations of current CPS security technologies.

Required Textbooks and Materials

No textbook required. Course materials will be provided on the course website.

Suggested Course Materials

Instructor will post suggested resources and materials on the course website.

Course Topics (Tentative)

- CPS Hardware Organization
    - MCUs: Memory, CPU, IO
    - Industrial Control Systems
    - Robotic Vehicles (Drones)
    - Self-Driving Vehicles
    - Robotic Arms, Mobile Robots
    - Sensors and Actuators (IMU, GPS)
- CPS Software Systems
    - Network Communications (MAVLink, ROS)
    - Availability and Realtime-ness
    - Control Theory and Algorithms
    - Sensor Filters (EKF)
    - RV Control Systems (ArduPilot, PX4)
    - Self-Driving Systems (Autoware, Apolo)
    - Simulators (Gazebo, CARLA)
    - Machine Learning Components
- CPS Attacks and Defenses
    - Sensor Attacks (GPS Spoofing, Jamming, Signal Injection Attacks, EMI)
    - Software Attacks (Traditional Vulnerabilities, Control-related Vulnerabilities, Cyber-Physical Vulnerabilities combining both domains)
    - Network-related Attacks (CAN Bus Attacks, GCS/Control Hijacking, Recent Attacks on Satellites, Authentication-related/ROS Node Impersonation Attacks)
    - System Attacks (Driver Vulnerability Exploits, Process/Memory Isolation, Privilege Escalation, RTOS CVEs, Execution Timing Interference)
    - AI Attacks (Adversarial Examples on LIDAR, Camera Images, LLM Vulnerabilities on Robot Development/Configuration)

Course Project

Students will work on a hands-on course project throughout the semester. Each team will consist of 2-3 students.

Project topics are open to student proposals, subject to instructor approval. Example topics include:

- Designing Cyber-Physical Attacks on a Robotic Aerial Vehicle
- Exploiting Security Vulnerabilities in a Real-Time Operating System
- Attacking a Self-Driving System with Adversarial Examples

Each team will give three formal presentations during class meetings:

- Project Pitch Presentation
- Midterm Project Presentation
- Final Project Demo and Presentation

Each team must submit the following materials before the Final Project Demo and Presentation:

- Final Project Report
- Project Code and Demo Environment

Course Schedule (Tentative)

Week	Date	Topic (Tentative)	Project
1	8/26	Course Introduction	-
2	8/31, 9/2	CPS Hardware (MCUs, Sensors, Actuators)	-
3	9/7, 9/9	Industrial Control Systems	-
4	9/14, 9/16	Robotic Platforms, Autonomous Vehicles	-
5	9/21, 9/23	CPS Software Foundations	Project Pitch Presentation
6	9/28, 9/30	Communication Protocols, Real-Time Requirements	-
7	10/5, 10/7	Control Algorithms and Sensor Estimation, Autopilot Software	-
8	10/12, 10/14	MIDTERM WEEK (NO CLASS)	-
9	10/19, 10/21	SITL/HITL Simulators	Midterm Project Presentation
10	10/26, 10/28	Sensor Attacks and Defenses (Spoofing, Jamming, Signal Injection)	-

11	11/02, 11/04	Software/Network Attacks and Defenses	-
12	11/09, 11/11	System-Level Attacks and Defenses	-
13	11/16, 11/18	CLASS CANCELLED	-
14	11/23, 11/25	FALL BREAK	-
15	11/30, 12/02	AI Attacks and Defenses (Adversarial Examples, ML Vulnerabilities)	Final Project Demo and Presentation
16	12/07	Class Overview and Closing	-

Grading Policy (Tentative)

(including percentages for assignments, grade scale, etc.)

Evaluation		
Assignment	Paper Presentations (3-4 times per student over the semester)	20%
Course Project	Project Pitch Presentation (10%) Midterm Project Presentation (15%) Final Project Demo and Presentation (25%) Final Project Report, Code and Demo Environment (30%)	80%
Exams	No midterm or final exam	

Grading Scale

- Project presentations and materials will be evaluated on a 100-point scale (0-100).
- Late submission will be penalized 10 points per day (24-hour period).

Scaled Score (%)	Letter Equivalent
90.1-100	A
85.1-90	A-
80.1-85	B+
75.1-80	B
70.1-75	B-
65.1-70	C+
60.1-65	C
<= 60	F

COVID-19 Guidelines and Resources

The information contained in the following link lists the University's COVID-19 resources for students and instructors of record.

Please see http://go.utdallas.edu/syllabus-policies.

Classroom Conduct Requirements Related to Public Health Measures

UT Dallas will follow the public health and safety guidelines put forth by the Centers for Disease Control and Prevention (CDC), the Texas Department of State Health Services (DSHS), and local public health agencies that are in effect at that time during the Fall 2021 semester to the extent allowed by state governance. Texas Governor Greg Abbott's Executive Order GA-38 prohibits us from mandating vaccines and face coverings for UT Dallas employees, students, and members of the public on campus. However, we strongly encourage all Comets to get vaccinated and wear face coverings as recommended by the CDC. Check the Comets United: Latest Updates webpage for the latest guidance on the University's public health measures. Comets are expected to carry out Student Safety protocols in adherence to the Comet Commitment. Unvaccinated Comets will be expected to complete the Required Daily Health Screening. Those students who do not comply will be referred to the Office of Community Standards and Conduct for disciplinary action under the Student Code of Conduct – UTSP5003.

Class Attendance

The University's attendance policy requirement is that individual faculty set their course attendance requirements. Regular and punctual class attendance is expected. Students who fail to attend class regularly are inviting scholastic difficulty. In some courses, instructors may have special attendance requirements; these should be made known to students during the first week of classes. Faculty have the discretion to set an attendance policy for their in-person meetings, but the absences due to COVID-19 cannot be counted against a quarantined student.

Class Participation

Regular class participation is expected. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Recordings

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

NOTE: if the instructor records any part of the course, then the instructor will need to add the following syllabus statement:

The instructor may record meetings of this course. These recordings will be made available to all students registered for this class if the intent is to supplement the classroom experience. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an exception is allowed by law.

Off-campus Instruction and Course Activities

(Below is a description of any travel and/or risk-related activity associated with this course.)

Comet Creed

This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:

"As a Comet, I pledge honesty, integrity, and service in all that I do."

Academic Support Resources

The information contained in the following link lists the University's academic support resources for all students.

Please see http://go.utdallas.edu/academic-support-resources.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus. Please review the catalog sections regarding the credit/no credit or pass/fail grading option and withdrawal from class.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.