











Instructor Info

-  Z. Berkay Celik
-  Office Hrs: By appointment
-  Lawson 1187
-  <https://berkay.github.io>
-  zcelik@purdue.edu


Course Info

-  Prereq: Bachelor degree in Computer Science or equivalent.
-  MW
-  4:30-5:45
-  REC (Recitation Bldg) Rm 309

Recitations Info

-  No recitations.

TA Info

-  TA is not assigned.

Overview

In this course, we will study the latest research in the design of Internet of Things (IoT) and Cyber-Physical Systems (CPS) and methods for securing them. The course will provide foundations of safety and security of IoT/CPS and covers the topics of policy verification, approaches for designing safe and secure systems, techniques for detecting problems in conventional IoT/CPS design and repairing such problems. Example topics include the security of voice-controlled devices, IoT applications, edge computing, industrial control systems, and autonomous vehicles.

The course aims to motivate the exploration of new problems that advance the state-of-the-art; thus, the course will include reviewing recent papers from top-tier conferences. Students successfully completing this class will be able to evaluate the security of Internet of Things and Cyber-Physical systems in academic and commercial security, and will have rudimentary skills in security research.

Prerequisites

The course assumes knowledge of system programming, program analysis, and basic probability and mathematical statistics. You must be comfortable writing code to process and analyze code and data, and be familiar with basic algorithmic design and analysis.

Material

There is no official textbook for the class. Slides will be provided and reading materials for each topic will be assigned from research papers and the following references:

Recommended Texts

1. Security Engineering, Ross J. Anderson
2. Computer Security: Principles and Practice - William Stallings, Lawrie Brown
3. Computer Security: Art and Science - Matt Bishop.

(Tentative) Grading Scheme

The course will be graded in the following proportions:

- 50% Research project
- 30% Presentation
- 10% Class notes
- 10% Paper summaries

It is the responsibility of the students to frequently check this web-page for schedule, readings, and assignment changes. As the professor, I will attempt to announce any change to the class, but this web-page should be viewed as authoritative.

Grading Details

Research Project

Building on knowledge gained in class, the main deliverable from this course will be a course project. The students may work on research projects in groups and preferably complete a conference-quality report at the end of the semester. The paper's topic must be security-relevant and the student(s) must be a lead author. Projects teams may include groups of up to two students; yet, groups of greater size will be expected to make greater progress. Details of the milestones and content will be given in class with the other project details. I will advise each team/individual independently as needed. The project grade will be a combination of grades received for a number of milestone artifacts and the final conference-quality report. The project will be graded on novelty, depth, correctness, clarity of presentation, and effort. The projects will be presented in the final week.

Presentation

Each student will be required to present 1-3 lectures of a paper assigned to the class, depending on the course enrollment. Students should prepare a detailed lecture complete with detailed slides. The slides will be distributed via Blackboard. The course instructor will provide additional details on the first day of class. All presenters must use the course template for either keynote or powerpoint. Linux folks can use the powerpoint template with Open Office if they choose.

Class Notes

A team of students will be charged with writing notes synthesizing the content of the presentation and class discussion.

Paper Summary

Understanding research papers is a key task in computer science research. In this class, students will provide two-page reviews research papers assigned as background readings. Roughly one reviews will be due per week. These reviews are due at the beginning of class. Most of the course readings will come from seminal papers in the field. Links to these papers will be provided on the course page.

(Tentative) Course Schedule

Introduction (January 13-17)

Week 1	Logistics & Overview	IoT/CPS Security: A brief history and applications Celik et al. , Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities
--------	----------------------	--

IoT Device Security (January 20-24)

Week 2	January 20 (M) No Class	Alrawi et al. , SoK: Security Evaluation of Home-Based IoT Deployment Kumar et al. , All Things Considered: An Analysis of IoT Devices on Home Networks
--------	-------------------------	--

IoT Application Security (January 27-31)

Week 3	-	Zhou et al. , Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. Wang et al. , Charting the Attack Surface of Trigger-Action IoT Platforms
--------	---	---

IoT Application Security 2 (February 3-7)

Week 4	-	Wang et al. , Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps Sugawara et al. , Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems
--------	---	--

Edge Computing Security Issues (February 10-14)

Week 5	-	Yousefpour et al. , All one needs to know about fog computing and related edge computing paradigms A complete survey Zhang et al. , Edge Computing- A Primer (Chapters 1 and 2, available at Purdue Libraries) Moghaddam et al. , Fog and Edge Computing Principles and Paradigms (Chapters 2 and 3, available at Purdue Libraries)
--------	---	---

Machine Learning for IoT/CPS security (February 17-21)

Week 6	-	Li et al. , Adversarial camera stickers: A physical camera-based attack on deep learning systems Cao et al. , Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving
--------	---	--

Sensors/Actuators (February 24-28)

Week 7	-	Han et al. , Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing using Different Sensor Types Birnbach et al. , Peeves: Physical Event Verification in Smart Homes
--------	---	---

Midterm and Project Progress Reports (March 2-6)

Week 8	Project Progress Presentations	
--------	--------------------------------	--

Voice-Controlled Devices (March 9-13)

Week 9 – [Zhang et al.](#), Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems
[Moghaddam et al.](#), Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices

Spring Vacation (March 16-20)

Week 10 No Class

Attacks to Power Grid System (March 23-26)

Week 11 – [Huang et al.](#), Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks
—, TBD.

Autonomous Vehicle Security (March 30- April 3)

Week 12 – [Pese et al.](#), LibreCAN: Automated CAN Message Translator
[Arun et al.](#), Exploiting Consistency Among Heterogeneous Sensors for Vehicle Anomaly Detection

Fault Identification and Tolerance (April 6-10)

Week 13 – [Yen et al.](#), Detecting and identifying faulty IoT devices in smart home with context extraction
[Yen et al.](#), Rivulet: A Fault-Tolerant Platform for Smart-Home Applications

IoT/CPS Fuzzing (April 13-17)

Week 14 – [Kim et al.](#), RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing
[Zheng et al.](#), FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation

Program Analysis for Security (April 20-24)

Week 15 – [Chen et al.](#), Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System
[Huang et al.](#), Using Safety Properties to Generate Vulnerability Patches

Control Systems Security (April 27-May 1)

Week 16 – [Zhang et al.](#), Towards Automated Safety Vetting of PLC Code in Real-World Plants
[Faezi et al.](#), A Non-Invasive Side Channel Attack Against DNA Synthesis Machines

Final Exam (May 4-9)

— Review and Project Presentations

Course Policies

Missing or Late Work

The score for a late homework, a paper review, a missed quiz and exam is 0. Exceptions will be made in case of serious illness or bereavement. If a student has a planned absence for a class when an exam will be given, the student should make arrangement before the planned absence to take the exam early or take a makeup exam after returning to campus.

Grade Disputes

Feedback on graded material will be posted on Blackboard in as timely a manner as possible. Once feedback for a graded assignment is posted, you will have 1 week from the posting date to dispute a grade. No re-grade requests will be honored after 1 week from posting feedback.

Collaboration Policy

You are encouraged to discuss course materials and reading assignments, and homework assignments with each other in small groups (two to three people). You must list all discussants in your homework write-up. Discussion about homework assignments may include brainstorming and verbally discussing possible solution approaches, but must not go as far as one person telling others how to solve a problem. In addition, you must write-up your solutions by yourself, and you may not look at another student's homework write-up/solutions (whether partial or complete).

Conduct and Courtesy

Students are expected to maintain a professional and respectful classroom environment. This includes: silencing cellular phones, arriving on time for class, speaking respectfully to others and participating in class discussion. You may use non-disruptive personal electronics for the purpose class participation (e.g., taking notes).

Correspondence with the instructor: The best way to correspond in this class is by emailing the instructor. Please prefix all course-related emails with the string **CS-529** to help filter email. The instructor will make every effort to answer promptly (within 48 hours). However, replies could be delayed due to circumstances outside the instructor's control.

Academic Integrity

Behavior consistent with cheating, copying, and academic dishonesty is not tolerated. Depending on the severity, this may result in a zero score on the assignment or exam, and could result in a failing grade for the class or even expulsion. Purdue prohibits "dishonesty in connection with any University activity. Cheating, plagiarism, or knowingly furnishing false information to the University are examples of dishonesty." (Part 5, Section III-B-2-a, University Regulations) Furthermore, the University Senate has stipulated that "the commitment of acts of cheating, lying, and deceit in any of their diverse forms (such as the use of substitutes for taking examinations, the use of illegal cribs, plagiarism, and copying during examinations) is dishonest and must not be tolerated. Moreover, knowingly to aid and abet, directly or indirectly, other parties in committing dishonest acts is in itself dishonest." (University Senate Document 7218, December 15, 1972). You are expected to read both [Purdue's guide to academic integrity](#) and [Prof. Gene's Spafford's guide](#) as well. You are responsible for understanding their contents and how it applies to this class.

Posting Class Material: Posting material associated with this class (e.g., solutions to homework sets or exams) without the written permission of the instructor is forbidden and may be a violation of copyright.

Students with Disabilities

Purdue University is required to respond to the needs of the students with disabilities as outlined in both the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 through the provision of auxiliary aids and services that allow a student with a disability to fully access and participate in the programs, services, and activities at Purdue University. If you have a disability that requires special academic accommodation, please make an appointment to speak with the instructor within the first three (3) weeks of the semester in order to discuss any

adjustments. It is the student's responsibility to notify the [Disability Resource Center](#) of an impairment/condition that may require accommodations and/or classroom modifications. We cannot arrange special accommodations without confirmation from the Disability Resource Center.

Instructor Absence

The instructor might be away for a few classes. There will be a guest instructor for these classes. If we need to reschedule additional classes, we will do so on an as-needed basis.

Emergencies

In the event of a major campus emergency, course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances beyond the instructor's control. Relevant changes to this course will be posted onto the course website and/or announced via email. You are expected to read your purdue.edu email on a frequent basis. Emergency Preparedness: Emergency notification procedures are based on a simple concept: If you hear an alarm inside, proceed outside. If you hear a siren outside, proceed inside. Indoor Fire Alarms are meant to stop class or research and immediately evacuate the building. Proceed to your Emergency Assembly Area away from building doors. Remain outside until police, fire, or other emergency response personnel provide additional guidance or tell you it is safe to leave. All Hazards Outdoor Emergency Warning sirens mean to immediately seek shelter (Shelter in Place) in a safe location within the closest building. "Shelter in place" means seeking immediate shelter inside a building or University residence. This course of action may need to be taken during a tornado, a civil disturbance including a shooting or release of hazardous materials in the outside air. Once safely inside, find out more details about the emergency. Remain in place until police, fire, or other emergency response personnel provide additional guidance or tell you it is safe to leave. In both cases, you should seek additional clarifying information by all means possible: Purdue Home page, email alert, TV, radio, etc. [Review the Purdue Emergency Warning Notification System multi-communication layers](#). Please review the [Emergency Response Procedures](#). Please review the evacuation routes, exit points, emergency assembly area and shelter in place procedures and locations for our building. [Video resources](#) include a 20-minute active shooter awareness video that illustrates what to look for and how to prepare and react to this type of incident.

Violent Behavior Policy

Purdue University is committed to providing a safe and secure campus environment for members of the university community. Purdue strives to create an educational environment for students and a work environment for employees that promote educational and career goals. Violent Behavior impedes such goals. Therefore, Violent Behavior is prohibited in or on any University Facility or while participating in any university activity.

CAPS Information

Purdue University is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, such individuals should contact [Counseling and Psychological Services \(CAPS\)](#) at (765)494-6995 during and after hours, on weekends and holidays, or through its counselors physically located in the Purdue University Student Health Center (PUSH) during business hours.

Nondiscrimination

Purdue University is committed to maintaining a community which recognizes and values the inherent worth and dignity of every person; fosters tolerance, sensitivity, understanding, and mutual respect among its members; and encourages each individual to strive to reach his or her own potential. In pursuit of its goal of academic excellence, the University seeks to develop and nurture diversity. The University believes that diversity among its many members strengthens the institution, stimulates creativity, promotes the exchange of ideas, and enriches campus life. Purdue University prohibits discrimination against any member of the University community on the basis of race, religion, color, sex, age, national origin or ancestry, marital status, parental status, sexual orientation, disability, or status as a veteran. The University will conduct its programs, services and activities consistent with applicable federal, state and local laws, regulations and orders and in conformance with the procedures and limitations as set forth in Executive Memorandum No. D-1, which provides specific contractual rights and remedies.