PURDUE UNIVERSITY

CS 59200-ICS: IoT/CPS Security (Spring 2022)

Instructor Info

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

Course Info

- Prereq: Bachelor degree in Computer Science or equivalent.
- TBD
- TBD
- TBD

Recitations Info

- No recitations.

TA Info

- TBD

Overview

This course will introduce the foundation of system security on the design of secure Internet of Things (IoT) and Cyber-Physical Systems (CPS). We will study the techniques for safety and security of IoT/CPS covering topics from formal verification approaches for policy validation, program analysis techniques for detecting problems in conventional IoT/CPS design and program repairing techniques to prevent and mitigate such problems. Example domains that we will study include the security of industrial control systems, (autonomous) vehicles, robotic vehicles, voice-controlled devices, and commodity IoT. This course aims to provide a systematic understanding of the field, and motivate the exploration of new problems that advance the state-of-the-art. Students successfully completing this class will be able to evaluate the security of academic and commercial IoT and CPS applications, and will have rudimentary skills in systems 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 (Python, C/C++), 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:

- 40% Research project (Presentation and Report)
- 20% Paper Presentations
- 10% Paper Reviews
- 30% Assignments

It is the responsibility of the students to frequently check this web-page for schedule, mandatory 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.

Assignments

Homework assignments (along with instructions) will be posted on the BrightSpace. There will be two or three homework assignments (both implementation/empirical and problem solving/mathematical). Each homework write-up must be neatly typeset as a PDF document. You can use LaTeX or any other system that produces typesetting of equal quality and legibility (especially for mathematical symbols and expressions). The pdf and code for assignments will be uploaded to BrightSpace.

Paper Presentations

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 BrightSpace. 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.

Paper Reviews

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.

CS 592 IoT/CPS Security Spring 2022

Date	Week	Topics	Mandatory Reading
1/10/2022	1	Course Logistics Security Basics	(1) Security Engineering (Book), Chapters 1, 2, 3 (2) Operating System Security (Book), Chapter 1
1/17/2022	2	IoT and CPS System Architecture: Their Differences, Understanding Their Threat Models	(1) NIST Special Publication: Cyber-Physical Systems and Internet of Things
1/24/2022	3	Program Analysis for IoT/CPS (Dynamic, Static Analysis, Symbolic Execution)	(1) Static Program Analysis (Book), Chapter 1 (2) Compilers, Principles, Techniques and Tools (Dragon Book), Chapter 10 (3) Celik et al., Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities (4) What is soundness (in static analysis) https://tinyurl.com/749mt8n8
1/31/2022	4	Building Blocks of Binary Analysis (Program Slicing, Taint Tracking, Summarization, Binary Rewriting, Symbolic Execution), Binary Hardening, Information Leaks, and Side-channels.	(1) Shoshitaishvili et al., (State of) The Art of War: Offensive Techniques in Binary Analysis
2/7/2022	5	Fuzzing for Discovering Software and Logic Bugs	(1) Software Security Principles, Policies, and Protection (Book), Chapter 4 Memory and Type Safety (2) Manes et al., The Art, Science, and Engineering of Fuzzing: A Survey (Paper) (3) Klees et al., Evaluating Fuzz Testing (Paper)
2/14/2022	6	Formal Analysis and Verification (Model Checking and Falsification with LTL/MTL)	(1) Kapinski et al., Simulation-Based Approaches for Verification of Embedded Control Systems (2) Logic in Computer Science, Modelling and Reasoning about Systems, Chapter 3 (Verification by Model Checking)
2/21/2022	7	Defense Strategies, Static and Dynamic Enforcers	(1) Software Security Principles, Policies, and Protection (Book), Chapter 5 Defense Strategies (2) Specification-based attacks and defenses in sequential control systems (Thesis), Chapters 1, 2
2/28/2022	8	Machine Learning for Perception and Decision Making (Autonomous Vehicle Controller Pipeline, Sensor Fusion, Kalman Filter)	(1) Yurtsever et al., A Survey of Autonomous Driving: Common Practices and Emerging Technologies (Paper)
3/7/2022	9	Models of Autonomous Systems, Data-driven Verification, Verification of Models with Black-box Components	(1) Formal Methods for Safe Autonomy: Data-driven Verification, Synthesis, and Applications (Thesis), Chapters 3, 4, 6
3/14/2022	10	**Spring Break**	
3/21/2022	11	**Research Progress Presentations**	
3/28/2022	12	Side Channel Attacks; Definition, Attack Types, Threat Model	(1) Spreitzer et al. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices
4/4/2022	13	Voice-assistant Systems, Their Architectures, Integrated Algorithms (Voice Recognition, Intent Extraction, Conflict Resolution)	(1) Lentzsch et al., Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem
4/11/2022	14	Security Protocols and Their Verification	(1) Blanchet et al., Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif (2) Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3
4/18/2022	15	Trusted and Confidential Computing (TCC)	(1) Cerdeira et al., SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems
4/25/2022	16	**Final Research Project Presentations**	
4/30/2022		**Classes end**	
2-7 May 2022		**Deadline for Final Projects**	

Each week, we will cover example IoT/CPS system architectures and papers from one of the following domains: (1) Commodity IoT, (2) Voice Assistant Systems, (3) Autonomous Vehicles (AV), (4) Robotic Vehicles (Drones and Swarms), (5) Industrial Control Systems, (6) Chemical Plants, and (7) Water Treatment Plants

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-592ICS** 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 mean 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.