PURDUE
UNIVERSITY™

Instructor Info

Z. Berkay Celik

Office Hrs: TBD

Lawson 1187

https://beerkay.github.io

zcelik@purdue.edu

Course Info

Monday & Wednesday

4:30 - 5:45pm (EST)

Online

TA Info

TBA

Office Hrs: TBA

Online

TBA

CS 426 - Computer Security

Overview

This introductory undergraduate course focuses on the principles and foundations of building secure computer systems, security best practices, and security failures in existing and emerging computer networks and systems. The course covers three key topic areas: basics of cryptography and crypto protocols, network security, and systems security. Students successfully completing this class will be able to understand and assess security threats, become familiar with security engineering best practices, and write better software, protocols and systems, and will have rudimentary skills in security research.

Catelog Description: The course focuses on the principles and foundations of building secure computer systems and on security and privacy challenges in existing and emerging computer networks and systems.

The course compares and analyzes security and privacy threats and architectures from an adversarial standpoint to understand how to build more secure protocols that can withstand ever-adaptive attacks.

Prerequisites

Undergraduate level CS 35400 Minimum Grade of C [may be taken concurrently] or (Undergraduate level ECE 46900 Minimum Grade of C or Undergraduate level EE 46900 Minimum Grade of C)

Material

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

Recommended Texts

1. Security Engineering – Ross Anderson, Third Edition
2. Computer Security and the Internet: Tools and Jewels – Paul C. Van Oorschot, Springer, 2nd edition

Announcements

Course announcements will be made through the course Brightspace page. Brightspace uses your Purdue e-mail address. You are expected to check this account regularly for information related to the class. Please sign-up on Campuswire to ask/answer questions. We will send class announcements through this site.

(Tentative) Grading Scheme

The course will be graded on assignments, exams, research project, and class participation in the following proportions:

- 50% Homework
- 15% Midterm Exam
- 15% Final Exam
- 15% Research Project
- 5% Class participation (quizzes)

How I Conduct this Class

I will post slides and videos under each week's module, as well as videos that will go through the slides and notes the way I would in class. Please remember that all class content is subject to copyright laws and should not be used for anything other than your own personal use in the course.

Requirements and Grading

Homework Assignments

There will be 4 or 5 graded homework assignments (both coding/implementation/empirical and problem solving/mathematical). Homework must be uploaded to Gradescope by the stated deadline.

Homework should be neatly typed using Latex, MS Word, or any text editor of comparable quality. Only PDFs are accepted on Gradescope. Figures, diagrams, and complex mathematical notations can be handwritten and included in the PDF as an image, but illegible solutions will receive no credit. The definitions of "complex" and "illegible" are at the discretion of the grader. You can use LaTeX or any other system that produces typesetting of equal quality and legibility (especially for mathematical symbols and expressions).

Please write your solutions as succinctly as possible while including all the necessary details. Please ensure that the following appear at the top of the first page of the write-up: **your name**, **your Purdue ID**, and **the ID's of any students** with whom you discussed the assignment. It is your responsibility to ensure that the submission is successfully received by Brightspace/Gradescope.

Exams

There will be a midterm and a final exam. All exams may be cumulative (i.e., they may cover any material covered in class up to that point in the session), and all exams are closed-book and closed-note.

Research Project

Building on knowledge gained in class, a deliverable of 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. Project 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.

Quizzes

There will be about 3-5 random quizzes during the semester that will mostly contribute to 5% attendance. Each quiz will be based on the most recent lecture and reading assignments. Please make sure you carefully read the assigned material for each lecture.

Missing or Late Work

The score for late homework, a missed quiz, and an exam is 0. Exceptions will be made in case of serious illness or bereavement. If a student has a planned absence from a class when an exam will be given, the student should make arrangements 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 Gradescope 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.

Course Policies

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-426** 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.

(Tentative) Topics

This introductory course will cover the following topics associated with computer security and privacy. A detailed list of lecture-by-lecture contents, assignments, and due dates (subject to change as the semester evolves) is available on the course schedule on Brightspace.

1. Preliminaries
   - Course Introduction
   - Security Fundamentals
     (a) Security Foundations: CIA of Security
     (b) Security Foundations: Types of Attackers
     (c) Security Foundations: Security Principles

2. Topic: Crypto and Crypto Protocols
   (a) Hashes and Message Authentication
   (b) Asymmetric Cryptography
   (c) Key Management
   (d) User Authentication
   (e) Authentication Protocols

3. Topic: Network Security
   (a) Networking Background and TCP Attacks
   (b) Transport Layer Security
   (c) Routing Security
   (d) DNS Security
   (e) Firewalls and Tunnels
   (f) Intrusion Detection Systems

4. Topic: Systems Security
   (a) Software Vulnerabilities
   (b) Access Control
   (c) Operating System Security
   (d) Web Security
   (e) Mobile Security
   (f) IoT Security
   (g) Machine Learning for Security Applications
   (h) Security of Machine Learning Systems