Cyber-physical System Security

CIS 4930/6930 (Special Topics in CISE)

Class Periods:

Tuesday - Period 4 (10:40 AM - 11:30 AM)

Thursday - Period 4 - 5 (10:40 AM - 12:35 PM)

Location:

Tuesday - TURL005

Thursday - FLG0260

Academic Term: Fall 2024

Instructor:

Prof. Sara Rampazzi - srampazzi (at) ufl (dot) edu

Office Hours: Tuesday 2:00 – 3:00 PM or by email appointment.

Teaching Assistant/Peer Mentor/Supervised Teaching Student:

Please contact through the Canvas website

Jennifer Sheldon – jsheldon (at) ufl (dot) edu

Office Hours: TBD

Course Description

Total Credit: 3.

Covers foundational concepts of cyber-physical system security. In particular, hardware and software threats and mitigation strategies of integrating sensing and actuation, AI computation, infrastructure control, and networking. Students will analyze research papers, write technical essays, present security research problems, conduct hands-on testing, and learn the challenges of building secure systems.

Course Pre-Requisites / Co-Requisites

COP 3530 (Data Structures and Algorithms) or instructor permission. Programming experience recommended.

Course Objectives

Successful students will have learned foundational concepts of cyber-physical system security and privacy and be able to:

- explain various types of cyber-physical system security and privacy threats;
- describe and differentiate threat models and attackers' capabilities under different scenarios;
- describe concepts and techniques of Life-Cycle Security, Software Assurance and Security Risk Analysis
- differentiate mitigation techniques and choose the appropriate techniques under specific scenarios;
- read, analyze, and learn methodologies for reproducible security research;
- demonstrate basic ability to formulate, write, and present research security problems;

In addition, successful students will have acquired experience in simulating attacks and defense strategies which include analyzing radio frequency signals and frequency spectrum using popular frameworks, and using pre-trained machine learning models and datasets.

Materials and Supply Fees

None.

Required Textbooks and Software

The material (e.g., slides, research papers, notes, demo equipment) necessary for the course will be provided by the instructor. The students can use their laptops/tablets to follow the lecture material during class.

Recommended Materials

- Bruce Schneier, "The Security Mindset": https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

- "Cyber-Physical Systems": https://ptolemy.berkeley.edu/projects/cps/
- S. Keshav, "How to Read a Paper": https://web.stanford.edu/class/ee384m/Handouts/HowtoReadPaper.pdf
- "The Mayfield Handbook of Technical and Scientific Writing": http://www.mit.edu/course/21/21.guide/

Required Computer

UF student computing requirement: *https://news.it.ufl.edu/education/student-computing-requirements-for-uf/*
The lab activities require a computer. Windows or Linux machines are recommended. Configurations for Mac can also be used with additional effort.

Course Schedule

Might change depending on time constraints and external events. Canvas will be used for announcements.

First Module: Introduction to cyber-physical security and privacy

Week 1:	Introduction to Cyber-physical system security fundamental concepts	
Week 2:	Security Risk Analysis, Life-Cycle Security, Software Assurance	
Week 3:	QA/Functional Testing and Software Security Analysis	Quiz 1
Week 4:	Research work analysis and vulnerability characteristics	
Week 5:	Vulnerability classification and responsible disclosure	Quiz 2
Week 6:	Encryption concepts and side-channel analysis	
Week 7:	Covert channels and root causes analysis	Quiz 3
Week 8:	Mitigation techniques and Secure Programming Practices	
Week 9:	Privacy Enhancement Technologies	Quiz 4

Second Module: Applied cyber-physical security

Week 10:	Laboratory 1: Physical sensor attacks and defenses	Lab assignment 1
Week 11:	Discussion session	Group assignment 1
Week 12:	Laboratory 2: Physical adversarial attacks and defenses	Lab assignment 2
Week 13:	Discussion session	Group assignment 2
Week 14:	Discussion session	Group assignment 3
Week 15	Thanksgiving break	
Week 16:	Special topic lectures	

Important Dates

12/10/2024 @ 3:00 PM Final Project Due

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is strongly recommended but not mandatory. Due to the course format, students who miss many lectures will be at a significant disadvantage. Laboratory assignments should be submitted in class.

Live demos/laboratories/Discussion sessions in class will not be recorded. The class lectures will be available in synchronous remote modality via Zoom (HyFlex) and available on the UF E-Learning platform after each lecture (Disclaimer: Recordings are made by the zoom platform, and it is not guarantee the quality or availability of the recording. To ensure that you view the complete lecture, attend the live lecture session.)

Notice: The lectures will be audio-visually recorded for students in the course to reference after the live recorded session. Students who choose to participate with their camera engaged or utilize a profile image are agreeing to have their video or image recorded. If you are unwilling to consent to have your profile or video image recorded, be sure to keep your camera off and do not use a profile image. A textual "chat" feature is also available during lectures, and it will be also recorded. Please note, since the lecture is in a public setting, chat messages may or may not be answerable during the live lecture.

Students are expected to have done the reading before class, complete the assignments on time, and actively participate during lectures and open discussions (e.g., by asking questions or by volunteering their opinions).

Quizzes submission: There are no makeups for missed or late submission quizzes (and the grade will be 0), but the lowest grade will be dropped at the end of the course.

Group assignment submission: Late submissions will have ten points deducted per day (rounded up for partial days) after the due date until the assignment closes. After closing, no work will be accepted (and the grade will be 0). Each group listed in the calendar provided by the instructor should participate in the discussion session in class. If the group that is in charge of presenting (Role 1) is not available during the scheduled presentation day, **the grade will be zero**, even if the slides were submitted on time. If none of the group members (from all the roles different from Role 1) is present to answer the questions, **10 points will be deducted** from the group grade.
There are no makeups for missed or late submission assignments.

Laboratory assignment submission: the assignment submission should be finalized and submitted during class time. There are no makeups for missed or late submissions.

Project submission: Late submissions will have ten points deducted for day (rounded up for partial days) after the due date until the project submission is closed. After closing, no work will be accepted (and the grade will be 0).

Excused absences must be in compliance with university policies and require appropriate documentation. If the student is not able to submit the assignments for a legitimate reason (e.g., medical or travel for UF purposes), students should contact the instructor and provide appropriate **documentation** a **few days ahead** of the assignment due date. Emergency situations should be notified to the instructor or the TA **before** the start of the class.

Excused absences must be consistent with university policies in the Graduate Catalog (https://catalog.ufl.edu/graduate/regulations) and require appropriate documentation. Additional information can be found here: https://gradcatalog.ufl.edu/graduate/regulations/

Expectations, Graduate/Undergraduate Co-listing
This course is a co-listed graduate/undergraduate course. Undergraduates are expected to register for CIS4930 whereas graduate students register for CIS6930.
Note: this course is primarily aimed at advanced undergraduates and graduate students!

There are 4 quizzes, 3 group assignments, and 2 laboratory assignments in this course. The class format for both graduate/undergraduate versions of the course is the same in terms of materials and assignments schedule. However, to ensure that graduate students do graduate-level work (and undergraduate students are not held to the standard for graduate students), students enrolled in CIS 6930 should complete additional advanced tasks for the laboratory assignments and for the final project (see Quizzes, Assignments & Project for the details).

Quizzes, Assignments & Project
Online quizzes will be used to evaluate the student's knowledge regarding the topics covered in the first module of the class. Quizzes will be announced in class and handled through the E-learning platform.

The **group assignments** for the second module will be written group assignments (with groups consisting of 4-5 people). Every group will choose one of the topics from a provided reading list of published works, complete the related written assignment, and present their findings in class following a presentation calendar provided by the instructor. Students are expected to have done the reading before class, submit the group assignments in time, and present their findings in class for open discussion. The assignments will be announced in class and handled through the UF E-Learning platform.

Laboratory assignments will consist of applied simulations of attacks and defense strategies. The students divided into groups are expected to analyze code and use frameworks to solve the given assignment during class time. Each laboratory assignment is composed of 4 tasks.

Students taking CIS 4930 must complete three tasks for each assignment to get full credit. Students taking CIS 6930 must complete all four tasks to get full credit. Students taking CIS 4930 are expected to solve the three tasks by analyzing the provided codebase and running given simulations of attacks and defense strategies. The students enrolled in CIS 4930 will acquire knowledge of state-of-art attacks and defense methodologies.

There is no final exam, but a **final project** done individually. The final project will consist of writing a short paper on one of the topics covered in a provided list for student taking CIS 4930. Students taking CIS 6930 must complete a review project to get full credit.

Questions are encouraged during class. Try to formulate the question before asking it and wait to see if it is answered in a few minutes so we can maintain flow. Lengthy discussions will be deferred to office hours.

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Group assignments (3)	100 each	25%
Quizzes (4)	100 each	15%
Laboratories (2)	100 each	20%
Final Project	100	40%
		100%

Grading Policy

(Might change. Canvas will be used for announcements.)

Percent	Grade	Grade Points
92.0 - 100.0	A	4.00
85.0 - 91.9	A-	3.67
78.0 - 84.9	B+	3.33
71.0 – 77.9	B	3.00
64.0 - 70.9	B-	2.67
57.0 - 63.9	C+	2.33
50.0 – 56.9	C	2.00
43.0 - 49.9	C-	1.67
36.0 - 42.9	D+	1.33
29.0 - 35.9	D	1.00
22.0 - 28.9	D-	0.67
0 - 21.9	E	0.00

More information on UF grading policy may be found at:
UF Graduate Catalog
Grades and Grading Policies

Academic Integrity

Students are required to follow the university guidelines on academic conduct and the student honor code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code) at all times. Students failing to meet these standards will be reported to the Dean of Students, which can result in the student receiving an 'E' for the course. In particular, students are explicitly forbidden from copying anything off of the Internet (e.g., source code,

text, slides) without proper attribution or citation. Students are also forbidden from copying code/answers from each other for the purposes of completing any assignment/quiz.

Ethics Statement

This course covers topics concerning the security of many systems that are widely deployed and potentially critical. Unethical use of the above technologies includes the circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services.

The students must respect the privacy and property rights of others at all times, or else will result in **failing the course**. The students must carefully read the Computer Fraud and Abuse Act (CFAA): https://www.nacdl.org/Landing/ComputerFraudandAbuseAct. This is one of several laws that govern "hacking." It is student responsibility to understand what applicable law prohibits.

The course is **NOT** a class on hacking. Any activity outside of the spirit of these guidelines will be reported to the proper authorities both within and outside of UF and may result in dismissal from the class and the University. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through the proper channels; however, students with any doubt should consult the instructor for advice. **DO NOT** conduct any action which could be perceived as technology misuse anywhere or under any circumstances.

As members of the university, students must review the university's policy on Responsible Use of Information Resources for guidelines concerning proper use of information technology at UF, as well as the UF Honor Pledge.

Students Requiring Accommodations

Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation

Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

In-Class Recording

Students are allowed to record video or audio of class lectures. However, the purposes for which these recordings may be used are strictly controlled. The only allowable purposes are (1) for personal educational use, (2) in connection with a complaint to the university, or (3) as evidence in, or in preparation for, a criminal or civil proceeding. All other purposes are prohibited. Specifically, students may not publish recorded lectures without the written consent of the instructor.

A "class lecture" is an educational presentation intended to inform or teach enrolled students about a particular subject, including any instructor-led discussions that form part of the presentation, and delivered by any instructor hired or appointed by the University, or by a guest instructor, as part of a University of Florida course. A class lecture does not include lab sessions, student presentations, clinical presentations such as patient history, academic exercises involving solely student participation, assessments (quizzes, tests, exams), field trips, private conversations between students in the class or between a student and the faculty or lecturer during a class session. Publication without permission of the instructor is prohibited. To "publish" means to share, transmit, circulate, distribute, or provide access to a recording, regardless of format or medium, to another person (or persons), including but not limited to another student within the same class section. Additionally, a recording, or transcript of a recording, is considered published if it is posted on or uploaded to, in whole or in part, any media platform, including but not limited to social media, book, magazine, newspaper, leaflet, or third party note/tutoring services. A student who publishes a recording without written consent may be subject to a civil cause of action instituted by

a person injured by the publication and/or discipline under UF Regulation 4.040 Student Honor Code and Student Conduct Code.

University Honesty Policy

UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/process/student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

The Herbert Wertheim College of Engineering values varied perspectives and lived experiences within our community and is committed to supporting the University's core values, including the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of race, creed, color, religion, age, disability, sex, sexual orientation, gender identity and expression, marital status, national origin, political opinions or affiliations, genetic information, and veteran status.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Coordinator
- HWCOE Human Resources, 352-392-0904, student-support-hr@eng.ufl.edu
- Pam Dickrell, Associate Dean of Student Affairs, 352-392-2177, pld@ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:

Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: https://counseling.ufl.edu, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence

If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://elearning.ufl.edu/.

Career Connections Center, Reitz Union, 392-1601. Career assistance and counseling; https://career.ufl.edu.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/;https://care.dso.ufl.edu.

On-Line Students Complaints*: https://distance.ufl.edu/getting-help/; https://distance.ufl.edu/state-authorization-status/#student-complaint.*