EEL 4930/5930 Cyber-Physical Systems Security

Spring 2019

Instructor:	C. Harrys Konstantinou	**Time:**	TR 11am-12.15pm
Email:	konstantinou@eng.famu.fsu.edu	**Place:**	A125
Course webpage:	eng.famu.fsu.edu/ konstantinou/cps	**Office:**	B-371

Course Description: The course covers introductory topics in security at both the physical layer and the cyber layer of Cyber-Physical Systems (CPS) (especially smart grid systems). The main objective of the course is to expose students to fundamental information security primitives and to understand the challenges in designing and securing CPS. Students will investigate different techniques used to model and analyze industrial CPS processes.

Objectives: To understand the issues in designing and analyzing CPS, what makes CPS hard to secure, common methods used to secure CPS, and the differences between securing traditional enterprise systems and industrial CPS. To investigate system design, monitoring, scheduling, management and control issues in the full lifecycle of CPS design and implementation. To develop the ability to interact with CPS components, learn CPS protocols, perform vulnerability assessment on CPS protocols and systems, design CPS and architectures that are resilient to attacks.

Prerequisites: The course is largely self-contained and will introduce the necessary technologies required for a qualitative (rather than quantitative) understanding of the security landscape of industrial CPS. Undergraduate/graduate courses in power systems, computer architecture, networking, and programming are preferred but not required. It is assumed that the students are familiar with some programming language, such as C, C++, Python, or MATLAB.

Office Hours:

- Before class (9.30am - 11am), or
- Other times by appointment only.

Main References:

- Instructor's lecture notes and handouts.
- A number of relevant papers from recent journal publications and conference proceedings will be discussed.
- There is no mandated textbook. Recommended books are:
  - "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems" by E. D. Knapp and J. T. Langill.
  - "Cyber-Physical Attacks: A Growing Invisible Threat" by G. Loukas.

Grading Policy:

- Paper summaries (10%).
- Online Active Participation (10%).
- Final Exam (5%).
- 2 Mini Projects/Assignments (15%).
- Project* (60%).

Extra bonus credit 10% for class participation.

*To be agreed upon by the instructor.
Note: Graduate students' reports must be in an IEEE-style paper for possible publications.

Grading Scale:

- A if $\geq$ 90%
- B if $\geq$ 80%
- C if $\geq$ 70%
- D if $\geq$ 60%
- F otherwise

Course Policy:

- Reading, analyzing, and discussing academic papers is a primary component of this course. To that end, each student is expected to read every paper and come to class prepared to discuss them.
- For the mini assignments students are expected to work independently. Offering and accepting solutions from others is an act of plagiarism, which will be penalized according to the Academic Honesty Policy. Discussion among students is encouraged, but when in doubt, students should direct their questions to the professor, tutor, or lab assistant.
- A topic will be assigned each week on Canvas and students are required to participate in the discussion boards. Participation is: 1) answering questions posed in the topic description, 2) answering questions posed by other students or the instructor, 3) posting interesting/insightful summaries on articles that pertain to the weeks coursework but not necessarily have to be on the topic. Participation is not: 1) simple two sentence responses, 2) linking to articles, 3), copying and pasting.
- The term project is a team project; each team can have up to 2 team members. Both members in each team will be graded equally for the project unless it has been verified that a student contributed significantly less.
- Class attendance: Both FAMU and FSU have a class attendance policy to comply with federal Title IV financial aid requirements. All students are required to attend classes regularly and be on time. Tardiness is no excuse and will be considered as being absent.
- Mandatory first day of classes attendance policy: Students who do not attend classes on the first day of classes may be dropped from their courses.
- You will not receive extensions, unless you contact me ahead of time and make the proper arrangements. Late assignments/projects/etc. will not be accepted.
- Last day to drop a course: Check with your University. No course drops will be allowed after this date except for: medical emergency, military service, administrative correction, and other (consult instructor).

Academic Honesty:
The full text of the Academic Honesty Policy is in the *Student Handbook*.

Resources:

- Undergraduate students: https://www.eng.famu.fsu.edu/undergraduate/student-handbook
- Graduate students: https://www.eng.famu.fsu.edu/ece/graduate/resources

ADA and Students with Disabilities:
Please see the Department and University for Details. Also please let me know if you have any special requirements.

Registring for this course means your agreement to this class policy and syllabus.

Course Outline:

- Week 1 (Jan 7): Overview, Intro to CPS, Security Mindset and Ethics
- Week 2 (Jan 14): Definitions, Design Principles, Threat Modeling, Real-time CPS
- Week 3 (Jan 21): CPS/ICS Security Characteristics, History, Threats, CPS/ICS operations
- Week 4 (Jan 28): Papers presentations and in-class assignment
- Week 5 (Feb 4): Cyber Infrastructure for the Smart Grid
- Week 6 (Feb 11): Cryptographic Basics
- Week 7 (Feb 18): Passwords, Authentication, Access Control & Papers presentations
- Week 8 (Feb 25): Network Attacks and Mitigations
- Week 9 (Mar 4): System Vulnerabilities and Security Mechanisms
- Week 10 (Mar 11): Attacking Utilities and Smart Devices
- Week 11 (Mar 18): Spring Break
- Week 12 (Mar 25): Papers presentations & Advanced Security Topics (State Estimation and FDI Attacks)
- Week 13 (Apr 1): Advanced Security Topics (Architectural Side Channel Attacks, Hardware Trojans)
- Week 14 (Apr 8): Advanced Security Topics (Physical Unclonable Functions, Hardware Performance Counters)
- Week 15 (Apr 15): Advanced Security Topics (Secure Multi-party Computation)& Final Exam
- Week 16 (Apr 22): Project presentations