

1. Course Number and Course Title:

COE694-01 Cyber-Physical System Security

2. Credit Hours:

3-0-3

3. Prerequisites and/or Co-Requisites:

Prerequisite: Approval of the CSE Head of Department

Co-requisites: None

Competencies: Software system development experience (for the project).

4. Name and Contact Information of Instructor:

Name: Dr. Mohammad Zulkernine

Email: TBA

Office: TBA

Phone: TBA

Office Hours: TBA

5. Course Description (Catalog Description):

Presents principles and practices for securing cyber-physical systems (CPSs). Explains CPS, Internet of Things, and security concepts by focusing on informational as well as software development aspects of CPSs. Covers key topics including dependable CPSs, security engineering for CPSs, CPS security analysis, and CPS network security. Studies the security of emerging CPS applications and domains such as autonomous and connected vehicles.

6. Textbook and other Supplemental Material:

Textbook:

- H. Song, G. Fink, S. Jeschke (Editors), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, Wiley - IEEE, 2017.

Other supplemental material:

- Ali, S., Al Balushi, T., Nadir, Z., Hussain, O.K., *Cyber Security for Cyber Physical Systems*, Springer, 2018.
- J.C. Laprie, *Dependability: Basic Concepts and Terminology*, Springer-Verlag, 1991.
- C. Pfleeger and S. Pfleeger, *Security in Computing*, Prentice-Hall, 2015.
- NIST, *Cyber-Physical Systems and Internet of Things*, National Institute of Standards and Technology (NIST) Special Publication 1900-202, March 2019.
- Recent Conference and Journal Papers (TBA).

7. Course Learning Outcomes:

Upon successful completion of the course a student will be able to:

1. Identify the importance of and issues with cyber-physical systems (CPSs) and security.

2. Review CPS dependability properties to address unique security and privacy challenges.
3. Apply strategies (tools and techniques) for mitigating security flaws in CPSs.
4. Design and implement secure CPSs by putting security into practice in different application areas of CPSs.
5. Evaluate CPSs with respect to security risks.
6. Critically review state of the art research work on CPS security.
7. Conduct independent research in the area of CPS security.

8. Teaching and Learning Methodologies:

Methods include lectures, project-based learning methods (research project, presentation), class discussions, and final exam.

9. Course Topics and Schedule:

Topic/Activity	Weeks
Introduction to CPS Security - I	Week #1
Introduction to CPS Security - II	Week #2
Background Paper Presentation (in class, individual)	Week #3
Dependability in CPS	Week #4
Security Engineering	Week #5
Background Paper Presentation (in class, individual)	Week #6
Software Security	Week #7
Cyber and Physical Security	Week #8
Project Proposal Presentation (in class, group)	Week #9
CPS Layers and Attacks	Week #10
CPS Security Framework	Week #11
CPS Security Evaluation	Week #12
Applications: Connected and Autonomous Vehicles Security	Week #13
Review of Course Materials	Week #14
Final Project Presentation (in class, group)	Week #15
Final Exam	Week #16

10. Schedule of Laboratory and other Non-Lecture Sessions:

This course has no labs.

The background papers should be presented individually, and these papers (published in the last 3-4 years) must be about cyber-physical system security and may be related to the proposed project.

The project proposal is required to be presented in a group in the class. The 4-page proposal prepared by the group should describe the project scope, motivation, research challenges, and milestones.

The research project may be conducted by a team of 2-3 students and should be delivered at the end of the semester. Based on the project work, a final report should be submitted. The 8-page report (including materials from the previously submitted proposal) may be similar to a conference/workshop paper describing motivations, methodology, and qualitative or quantitative evaluation of the project work.

11. Out-of-Class Assignments with Due Dates:

Assignment	Due Date
Background paper presentation (individual)	Weeks #3, #6
Project proposal presentation (group)	Week #9
Project proposal submission (group)	Week #9
Final project presentation (group)	Week #15
Final project work submission (group)	Week #15
Final project report submission (group)	Week #15

12. Student Evaluation:

Assessment	Weight	Due Date
Class presentation	20%	Weeks #3, #6, #9, #15
Project proposal	10%	Week #9
Project work	20%	Week #15
Project report	10%	Week #15
Final exam	40%	Week #16

13. Assessment Instruments:

Assessment	Course Learning Outcomes
Class presentation	01, 06, 07
Project proposal	02-03
Project work	04-07
Project report	04-07
Final exam	01-05

14. Contribution of Course to Program Outcomes:

MSCOE Program Outcomes	Emphasis in this course	Course Learning Outcomes
1. Perform research emphasizing creativity, independent learning and scientific methods in a chosen area of computer engineering	•	01-04, 07

2. Apply advanced mathematics and engineering knowledge in identifying, formulating and solving engineering problems	●	03-05
3. Select and use techniques, skills and modern tools necessary for research or professional practice	●	03-05
4. Communicate effectively	◐	06-07
5. Recognize the need for and engage in life-long learning		
6. Attend to professional and ethical responsibilities		06

Emphasis: ● High; ◐ Medium; ○ Low; Blank – Nothing Specific Expect

15. Letter Grade Policy:

Letter Grade	Total Score (T)
A	$T \geq 93$
A-	$89 \leq T < 93$
B+	$84 \leq T < 89$
B	$80 \leq T < 84$
B-	$75 \leq T < 80$
C+	$70 \leq T < 75$
C	$66 \leq T < 70$
F	$T < 66$