Jordan University of Science and Technology

Faculty of Computer & Information Technology

Computer Engineering Department

CPE597 Special Topics In Computer Engineering

First Semester 2024-2025

Course Catalog
3 Credit Hours. This course is an introduction to machine learning covering supervised and unsupervised learning. Supervised learning will focus on regression problems and how algorithms, such as gradient descent, can be used for fitting model parameters. The course then moves to multiple classification algorithms, such as logistic regression, support vector machines, K-nearest neighbor. Example algorithms on dimensionality reduction, such as principal component analysis, will also be discussed. Artificial neural networks and their use in applications such as, image processing and natural language processing will also be covered. In the unsupervised learning, the course will focus on clustering. Throughout the course, students will write code to gain practice in applying the course concepts.
Teaching Method: Blended

Text Book	
Title	Principles of Secure Processor Architecture Design
Author(s)	Jakub Szefer
Edition	1st Edition
Short Name	1
Other Information	

Instructor	
Name	**Dr. Mazen AlWadi**
Office Location	M2 L2
Office Hours	
Email	mgalwadi@just.edu.jo

Class Schedule & Room

Section 1:
Lecture Time: Mon, Wed : 12:30 - 13:30
Room: CPE07-M7L2

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Week 1	Introduction to Secure Processor Architectures	
Week 2	Basic Computer Security Concepts	
Week 3	Secure Processor Architectures	
Weeks 4, 5	Trusted Execution Environments	
Week 6	Hardware Root of Trust	
Week 7	Memory Protections	
Weeks 8, 9	Multiprocessor and Many-Core Protections	
Weeks 10, 11	Side-Channel Threats and Protections	
Week 12	Security Verification of Processor Architectures	
Weeks 13, 14	Principles of Secure Processor Architecture Design	
Weeks 15, 16	Case Study	

Mapping of Course Outcomes to Program Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Understanding the challenges and requirements of securing the data in hardware [2A, 1B, 1C, 1E, 2SO1, 1SO2, 1SO6, 1SO7]	20%	
Learning the differences between different Trusted Execution Environments [1A, 1B, 1SO1, 1SO2, 1SO6, 1SO7]	20%	
Understanding the different hardware security features and how each one can be used to thwart specific attacks [1A, 1B, 1C, 1E, 1K, 1SO1, 1SO2, 1SO6, 1SO7]	30%	
Understanding the memory protection, side-channel attacks, and the multiprocessor and Many-core protection techniques. [1A, 1B, 1C, 1E, 1K, 1SO1, 1SO2, 1SO6, 1SO7]	30%	

Relationship to Program Student Outcomes (Out of 100%)																	
A	B	C	D	E	F	G	H	I	J	K	SO1	SO2	SO3	SO4	SO5	SO6	SO7
14	12	8.67		8.67						6.67	14	12				12	12

Evaluation

Assessment Tool	Weight
First exam	20%
Assignments, and quizzes	20%
Second exam	20%
Final Exam Theoretical	40%

Policy	
Attendance	Attendance will be recorded at the beginning of each class, and missing 20% of the classes results in automatic dismissal (No excuses). If a student misses a class, it is their sole responsibility to catchup.
Exams	No books or notes are allowed in the exams or quizzes. The exams and quizzes format may include multiple choice, but the most common is problem solving, analysis and design.
Makeups	Exam makeup requires online application within two days of the announced date, pending formal approval, makeups are arranged by the faculty for all courses in one day, typically one week after the exams period end.
Cheating	Copying assignments and cheating by any means in the exams and quizzes results in sever penalty .

Date Printed: 2024-10-03