Jordan University of Science and Technology

Faculty of Computer & Information Technology

Computer Information Systems Department

CIS745 Data - Driven Security - JNQF Level: 7
First Semester 2023-2024

Course Catalog
3 Credit Hours. The course aims at locking down networks, thwart malware, prevent hacks by improving visibility into the environment, using the power of data and security and by using data analysis and visualization. It demonstrates how to gather feedback, measure the effectiveness of security methods, and make good decisions based on data using hands-on approaches with real-world examples. The course covers topics such as how to acquire and prepare security data, correlate security events, use simple statistical methods to detect malware, predict rogue behavior, and more.

Text Book	
Title	Machine Learning in Cybersecurity
Author(s)	Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel
Edition	1st Edition
Short Name	Ref#1
Other Information	2020

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref#2	Computer Security: Principles and Practice	William Stallings and Lawrie Brown	3rd Edition	

Instructor	
Name	**Dr. Malik Qasaimeh**
Office Location	-
Office Hours	Sun : 12:30 - 14:30 Mon : 13:00 - 15:00 Tue : 12:30 - 13:30 Wed : 12:00 - 13:00
Email	mgqasaimeh@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Wed : 13:00 - 16:00 Room: A2120

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Weeks 1, 2, 3	Introduction to Cybersecurity 1	From **Ref#2**
Weeks 4, 5, 6	Introduction to Cybersecurity 2	From **Ref#2**
Weeks 7, 8	Security Design Principles	From **Ref#2**
Weeks 9, 10	Threat Modeling for Large System	From **Ref#1**, From **Ref#2**
Weeks 11, 12, 13	Machine Learning and Cybersecurity	From **Ref#1**
Weeks 14, 15	Adversarial Machine Learning in Cybersecurity	From **Ref#1**
Week 16	Selected articles in Security Analytics	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Students will learn to software security , including vulnerability identification, malware protection, and cyberattack prevention. [10K] [10L7K1]	10%	
Students will acquire the knowledge and skills needed to design secure systems and networks, applying security design principles. They will be capable of creating and implementing robust security measures to protect against threats. [20SO1] [20L7S1]	20%	
Students will develop expertise in conducting threat modeling for large-scale systems. They will be able to identify potential vulnerabilities and design security solutions to mitigate risks within complex environments. [10SO2] [10L7S3]	10%	
Students will be proficient in utilizing machine learning techniques for cybersecurity applications. They will understand how to apply machine learning algorithms to detect and respond to security threats effectively. [20SO2] [20L7S1]	20%	
Students will be equipped with the knowledge and techniques necessary to counter adversarial machine learning attacks in cybersecurity. They will be able to protect machine learning models and systems from adversarial manipulation. [20SO1] [20L7S3]	20%	
students will develop advanced research skills by critically evaluating selected articles in security analytics. They will be prepared to engage in cutting-edge research, contribute to the field, and stay updated on emerging cybersecurity trends. [20SO6] [20L7C4]	20%	

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
										10	40	30				20

Relationship to NQF Outcomes (Out of 100%)			
L7K1	L7S1	L7S3	L7C4
10	40	30	20

Policy	
Teaching & Learning Methods	? Class lectures: Class lectures will expose students to the knowledge required by this course ? Class Discussions: Relevant issues will be discussed in class. These discussions are supposed to improve the students? communication and problem solving skills by motivating them to express their opinions. ? Activity: Students will be expected to work on a group activity. The activity could be a small software project, or a case study of a healthcare provider. In addition to improving the students? technical and analytical skills, this project aims at improving the students? team work, self management, and planning and organizing skills. ? Self-study: Students will be required to study one of the assigned chapters as self-study. A number of questions from the self-study chapter will be included in the exam. This learning method aims at improving the students' learning skills.
Attendance	Excellent attendance is expected. In accordance with university regulations, students missing more than 20% of total classes are subject to failure. No excuses will be accepted. If you miss class, it is your responsibility to find out about any announcements or assignments you may have missed. Attendance will be recorded at the beginning or end of each class.
Participation	You are expected to participate in class. Participation includes asking and answering questions, raising issues, and suggesting solutions to the discussed problems.
Activity	Students are expected to work on an activity within a group of 3-4 students. The activity could be a small software project, or a case study of a healthcare provider.
Exams	All exams will be CLOSE-BOOK. The format for the exams is generally as follows: multiple-choice, and short essay questions.
Makeup Exams	Makeup exam should not be given unless there is a valid excuse. Arrangements to take an exam at a time different than the one scheduled MUST be made prior to the scheduled exam time. In accordance with university regulations, students should bring a valid excuse authenticated through valid channels in JUST.
Workload	Average work-load student should expect to spend is 4 hours/week.
Code of Conduct	Quizzes and exams need to be done individually. Copying of another student's work, even if changes are subsequently made, is inappropriate, and such work will not be accepted. Cheating or copying from neighbor on exam is an illegal and unethical activity and standard JUST policy will be applied. All graded assignments must be your own work.

Date Printed: 2023-10-29