Jordan University of Science and Technology
Faculty of Computer & Information Technology
Computer Information Systems Department

CIS 433 Information Security

Course Catalog

3 Credit hours (3 h lectures). The course covers classic security topics, such as applied cryptography, authentication, authorization and basic security principles. Furthermore, it covers some recent topics such as web security and virtual machines security. The topics that the course covers are listed below:

- **Overview:** Confidentiality, Integrity, Availability. Security policy and mechanism. Basic principles of secure system design.
- **Cryptography:** Basic crypto primitives, Secret key crypto, public key crypto, Digital signatures, Message authentication.
- **System security:** Authentication, Access Control, Discussion of popular systems and security protocols.
- **Network Security:** Firewalls, Intrusion Prevention Systems, DHCP spoofing and snooping, MAC flooding.

Course Information

Course Title	**Information Security**
Course Number	**CIS 433**
Prerequisites	**Statistics (Math131) & Data Structures (CIS 328)**
Course Website	

Text Book(s)

Title	Computer Security: Principles and Practice
Author(s)	William Stallings and Lawrie Brown
Publisher	Pearson Education
Year	2015
Book Website	https://www.pearsonhighered.com/program/Stallings-Computer-Security-Principles-and-Practice-3rd-Edition/PGM153489.html
Edition	3rd

References

Books	Security in Computing by Pfleeger, Pfleeger, Margulies. Prentice Hall, 2015, 5th ed
Internet links	https://www.pearsonhighered.com/program/Pfleeger-Security-in-Computing-5th-Edition/PGM25284.html

Instructors

Instructors	Dr. Qussai M. Yaseen
Office Location	Engineering Building N2 L0
Office Phone	Ext. 22399
E-mail	qmyaseen@just.edu.jo

Teaching Assistant
Ftoon abu Shaqrah

Class Schedule & Room				
Section	**Time**	**Days**	**Room**	**Instructor**
1	9:30 – 10:30	Sunday, Tuesday, Thursday	CIS01 Lab	Dr. Qussai Yaseen

Office Hours		
Instructor	**Days**	**Time**
Dr. Qussai Yaseen	Sunday, Tuesday, Thursday	10:30 -11:30
	Monday, Wednesday	11:30 – 12:30

Topics Covered

The schedule is subject to change depending upon the actual class dynamics and workflow during the semester

Topic	Chapters in Text	Related CLOs	Week No.
Introduction. Basic security principles.	Chapter 1	ILO 1	1
Cryptography: Simple symmetric-key ciphers. DES.	Chapter 2 + Chapter 20	ILO 7 ILO 5	2,3
Public-key cryptography and RSA, Diffie-Hellman.	Chapter 2 + Chapter 21	ILO 7 ILO 5	3, 4
User Authentication: Means of Authentication, Password-Based, Token-Based, Biometric, Remote User authentication. Security Issues for User Authentication.	Chapter 3	ILO 5 ILO 11	5
Access Control: Access Control Principles. Subjects, Objects and Access Rights. Discretionary Role-Based Access Control.	Chapter 4	ILO 5 ILO 3 ILO 11	6,7
Database and Cloud Security: Database Access Control. Inference. Database Encryption. Data Protection in the Cloud	Chapter 5	ILO 4 ILO 3 ILO 11	8,9
Malicious Software: Viruses. Worms. Bots. Rootkits.	Chapter 6	ILO 4 ILO 3 ILO 11	10,11
Intrusion Detection: Intruders. Intrusion Detection. Host-Based and Distributed Host-Based Intrusion Detection. Network-Based Intrusion Detection. Honeypots.	Chapter 8	ILO 4 ILO 3 ILO 11	12,13
Network Security, Firewalls and Intrusion Prevention Systems: Firewall Characteristics. Types of Firewalls. Firewall Location and Configurations. Intrusion Prevention Systems. MAC address Flooding, DHCP starvation and Spoofing.	Chapter 7 + 9	ILO 4 ILO 3 ILO 11	14,15

Course Objectives

No.	Course Learning Outcomes (CLOs)	Mapping CLOs to ABET POs	Assessment Methods
1	A successful student in this course will be able to be familiar with information security concepts and terms.	ILO 1	Exams
2	A successful student in this course will be able to use symmetric and asymmetric encryption methods.	ILO 7 ILO 5	Exams, Labs
3	A successful student in this course will be able to code a hacking system that teach students how attackers think and hack systems.	ILO 5 ILO 11	Project
4	A successful student in this course will be able to analyze access control methods and their differences, and implement an access control method.	ILO 3 ILO 5 ILO 11	Exams, Project
5	A successful student in this course will be able to design some types of malicious software.	ILO 4	Exams, Labs
6	A successful student in this course will be able to understand how countermeasures works and how intruders may bypass security countermeasures.	ILO 4	Exams, Labs

Relationship to Program Outcomes (score out of 5)														
Program Outcome	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Mapping Score	5		2	4	4		2				4			

Evaluation		
Assessment Tool	**Expected Due Date**	**Weight**
First Exam	TBD	15%
Second Exam	TBD	15%
Activity/ Assignment/Project	TBD	30%
Final Exam	TBD	40%

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.

Other Policies and Notes	
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.

Presentation on theme: "Computer Security: Principles and Practice"â€” Presentation transcriptÂ 3 Selecting Controls or Safeguards controls or safeguards are practices, procedures or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recover classes of controls: Management: focus on policies, planning Operational: address (correct) implementation Technical: correct uses of SW and hardware Given the results of some form of risk assessment. explore system and network security 5 Skill level: apprentice Hackers with minimal technical skill who primarily use existing attack toolkits â€¢ They likely comprise the largest number of attackers, including many criminal and activist attackers â€¢ Given their use of existing known tools, these attackers are the easiest to defend against â€¢ Also known as â€œscript-kiddiesâ€ due to their use of existing scripts (tools) â€¢.Â Used by analysis module to refine intrusion detection parameters and algorithms by security admin to improve protection 39

2. Computer security education, often termed information security education or information assurance education, has emerged as a national goal in the United States and other countries, with national defense and homeland security implications. The NSA/DHS National Center of Academic Excellence in Information Assurance/Cyber Defense is spearheading a government role in the development of standards for computer security education.Â The book highlights these principles and examines their application in specific areas of computer security. â€¢ Design approaches: The book examines alternative approaches to meeting specific computer security requirements. â€¢ Standards: Standards have come to assume an increasingly important, indeed dominant, role in this field.