Princess Sumaya University for Technology
The King Hussein School for Information Technology
Computer Science Department

ABET Course Syllabus – Fall Semester 2021/2022
11464 Information System Security

1. Course Information

Catalog Description	This course aims to provide a deep and comprehensive study of the security principles and practices of information systems. Topics include security threats, vulnerabilities and countermeasures, attacks, security services (confidentiality, integrity, availability, non-repudiation, accountability), cryptography: classical encryption techniques, block ciphers and stream ciphers, symmetric-key and asymmetric-key cryptography, authentication and digital signature, key management and cryptographic protocol, DES and AES, Block cipher operation modes, asymmetric ciphers: RSA, Diffie-Hellman key exchange, hash functions, MAC functions, digital signature: digital Signature Standard DSS, key management and distribution, X.509 certificates, user authentication, access control, security in operating systems, web security: SSL and TLS, electronic mail security (PGP. MOME), malicious software, and firewalls. At the end of this course, students are expected to be familiar with many of the basic principles and practices in information systems security. In particular, understand what the fundamental theory is behind information security, what the common threats are, what are the basic principles and techniques when designing a secure system, and how to gauge the protections and limitations provided by today's technology
Credit Hours	3
Prerequisite	CS11212 Data Structures and Introduction to Algorithms
Course Type	Lecture
Required/Elective	Required
Textbook	Computer Security: Principles and Practice 4/E, by William Stallings & Lawrie Brown. Pearson Press, ISBN 10: 1-292-22061-9, ISBN 13: 978-1-292-22061-1, 2018.
References	Cryptography and Network Security: Principles and Practice, 7th Edition by William Stallings. ISBN 10:1-292-15858-1 ISBN 13: 978-1-292-15858-7, 2017.
Instructor	Dr. Mustafa Al-Fayoumi Email: m.alfayoumi@psut.edu.jo Office: IT 307 Office Phone: 5359949 Ext: 5302
Class Schedule	Sun, Tue, Thu: 11:00 – 12:00
Class Location	1st Sec.: 303
Office Hours	TBA
Teaching Assistant	No

2. Course Contents

Week(s)	Topic(s)	Chapter in Text	Reference
1	**Overview of information systems Security**	Chapter 1	Ref. 1
	- Computer Security Concepts, - Threat, Attacks and Assets - The Main Pillars of Security (CIA) and some people add other Properties (authenticity, Authentication, Non-repudiation and accountability) - Fundamental Security Design Principles		
2-3	**Cryptography Tools**	Chapter 2	Ref. 1
	- Confidentiality with Symmetric Encryption - Message Authentication and Hash Functions - Public-key cryptosystems - Digital Signature and Key Management - Practical Application: Encryption of Stored Data		
3-6	**Cryptographic Algorithms Symmetric Ciphers**	Chapter 2	Ref. 2
	- Classical encryption techniques o Symmetric Cipher model- Cryptography and Cryptanalysis and brute-force Attack o Substitution Techniques ▪ Caesar Cipher – addition and multiplication ▪ Monoalphabetic Cipher – Digram and trigram ▪ Playfair Cipher ▪ Polyalphabetic Ciphers - Vigenère Cipher ▪ One-Time Pad o Transposition Techniques – rail fence and double - Modern Block Ciphers- Block Cipher Principles o Simplified DES o The Data Encryption Standard (DES) o Some math - finite fields o Advanced Encryption Standard (AES)		
6-9	**Asymmetric Ciphers**	Chapter 21	Ref. 1
	- More math - some number theory - Public-key cryptography: RSA - Diffie-Hellman key exchange scheme - Digital signature algorithms: DSA - Hybrid System		
9-10	**User Authentication**		
	- Types of authentication methods - Remote User -Authentication Using Symmetric Encryption - Remote User -Authentication Using Asymmetric Encryption	Chapter 3	Ref. 1
10-12	**Access control: Access - control principles and policies**	Chapter 4	Ref. 1

12-13	**Firewalls and Intrusion Prevention System (IPS)**	Chapter 9	Ref. 1
13-15	**Operating System Security**	Chapter 12	Ref. 1

3. Course Learning Outcomes (CLOs)

Upon completion of the course, students will be able to:

1. Describe the main security objectives and define basic security concepts and principles. **(@1))**
2. Demonstrate the ability to identify a variety of generic security threats, vulnerabilities, and attacks, and identify and analyze particular security problems for a given application (@2)
3. Analyses the common network vulnerabilities and attacks. (@2)
4. Apply mathematical foundations, algorithm principles, and computer science theory in topics such as cryptographic operations and security architecture. (@1)
5. Design, implement and evaluate a secure network system. (@2)

4. Assessment Policy

Assessment Tool	Expected Due Date	Weight
Participation, Home Works, Quizzes and Project	All Course duration	20%
First exam	TBA	20%
Second Exam	TBA	20%
Final Exam	16th week	40%

5. Contribution of the Course to the Professional Component

Computer Science Topics	100%
General Education	20%
Mathematics & Basic Sciences	40%

6. Expected level of proficiency from students entering the course

Mathematics	Some
Physics	Not applicable
Technical writing	Some
Computer programming	Some

7. Material available to students, instructors, TAs, and department at end of course

	Students	Department	Instructors	TA(s)
Course objectives and outcomes form	X	X	X	
Lecture notes, homework assignments, and solutions	X	X	X	
Samples of homework solutions from 3 students		X		
Samples of lab reports of 3 students		X		
Samples of exam solutions from 3 students		X		
Course performance form from student surveys		X	X	
End-of-course instructor survey		X	X	