هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

Course Specification

Course Title: Computer Data Security & privacy	
Course Code: 324 COMP-3	
Program: Bachelor in Computer Science	
Department: Computer Science	
College: College of Computer Science and Information Technology	
Institution: Jazan University	
Version: V2	
Last Revision Date: 12 September 2021	

Table of Contents:

A. General information about the course:

Course Identification					
1. Credit hours:	3				
2. Course type					
a.	University ☐	College ☐	Department☒	Track☐	Others☐
b.	Required ☒	Elective☐			
3. Level/year at which this course is offered:	11/4				

4. Course general Description

This course provides integrated, comprehensive and up-to-date coverage of topics in Computer Security. The list of topics covers the basics of Computer Security, Cryptographic Tools, User Authentication, Access Control, Malicious Software, Denial-of-Service Attacks, Intrusion Detection and Message authentication.

5. Pre-requirements for this course (if any):
None

6. Co- requirements for this course (if any):
None

7. Course Main Objective(s)

- Discuss the basic concepts and goals of Information Security and explain their relevance in various contexts.
- Explain the fundamental principles of access control models and techniques, authentication and secure system design.
- Describe different cryptographic protocols and techniques, respective strengths, weaknesses, application and implementation techniques.
- Illustrate the methods and techniques to be applied for intrusion detection and prevention.
- Familiarize students with various types of malicious software and attacks on information security and their countermeasures.

1. Teaching mode (**mark all that apply)**

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	44	80%
2.	E-learning		
3.	Hybrid		

No	Mode of Instruction	Contact Hours	Percentage
	- Traditional classroom - E-learning		
4.	Distance learning (Self Learning)	11	20%

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	22
2.	Laboratory/Studio	22
3.	Field	
4.	Tutorial	
5.	Others (specify)	8
	Total	52

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Define the basic terminology, encryption standards, techniques and concepts in the field of computer and data security.	K1	• Lectures/Presentations • Media Lectures	• Mid-Term Exam • Assignment- 1 • Final Theory Exam
1.2	Explain the implications of cryptography in terms of privacy, security and ethical issues, along with the latest developments in the field.	K2	• Lectures/Presentations • Media Lectures	• Mid-Term Exam • Assignment- 2 • Final Theory Exam
2.0	Skills			
2.1	Evaluate various cryptographic algorithms and protocols.	S2	• Lectures /Presentations • Media Lectures • Tutorials	• Assignment - 1 • Assignment – 2 • Final Theory Exam
2.2	Justify appropriate encryption standards and techniques to suit	S2	• Lectures /Presentations • Media Lectures	• Assignment - 1 • Assignment – 2

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
	specific business and technological needs.		• Tutorials	• Final Theory Exam
2.3	Analyze various types of malicious software, attacks and their countermeasures for information security.	S1	• Lectures /Presentations • Media Lectures • Tutorials	• Assignment -1 • Final Theory Exam
2.4	Develop mechanisms for information security, access control, authentication and intrusion detection to solve the specified security problem.	S3	• Lectures /Presentations • Lab Demonstration • Media Lectures • Group discussion	• Assignment - 2 • Lab Exam • Final Theory Exam
3.0	Values, autonomy, and responsibility			
3.1	Demonstrate the ability to work in a group to achieve common assignments and activities in the field of computer and data security.	V2	• Group Discussion	• Assignment – 2 (Group Assignment)

C. Course Content

No	List of Topics	Contact Hours
1.	Overview Definition of Computer Security, CIA triad, Challenges of Computer Security, Computer Security Terminology, Security Concepts and Relationships, System resource, Types of attacks, Countermeasures, Threat Consequences, Threat Actions, Network security attacks	3T + 3P
2.	Cryptographic Tools Major Achievements Symmetric encryption, cryptanalysis, brute-force attack, Symmetric Block Encryption Algorithms: DES, Triple DES, AES, Stream Cipher, Random and Pseudorandom numbers, Message authentication, message authentication code, One-way Hash Function, Message Authentication Using a One-Way Hash Function, Hash Function requirements, Secure Hash Function algorithms, Public-Key Encryption, RSA Public-Key encryption algorithm, Security of RSA, Diffie-Hellman Key Exchange Algorithm, Other Public-Key Cryptography	5T + 5P

	Self-Study Topic(s): Random and Pseudo-random numbers, Digital Envelopes, Man-in-the-middle attack	
3.	User Authentication Authentication process, Means of Authentication, Password-Based Authentication, Vulnerability of Passwords, Password Cracking, Password Selection Strategies, Token-Based Authentication, Biometric Authentication, Operation of a Biometric Authentication System, Security issues for User Authentication, Defenses Self-Study Topic(s): Hashed Passwords, Password File Access Control	3T + 3P
4.	Access Control Access Control, Access Control Policies, Access Rights, Discretionary Access Control, Role-based Access control, Attribute-based access control, identity management, credential management, access management	3T + 3P
5.	Malicious Software Malware, Types of Malware, Viruses: components, phases, Viruses Classification, Worms, State of Worm Technology, Clickjacking, Spam, Trojan Horse, Ransomware, Logic Bomb, Zombie, Botnet, Key-logger, Phishing and Identity Theft, Backdoor Rootkit, Malware Countermeasure Approaches Denial of Service Denial-of-service (DoS) attack, Nature of Denial-of-Service Attacks, Source Address Spoofing, SYN spoofing attack, Flooding attacks, Defenses against Denial-of-service attacks Self-Study Topic(s): State of Worm Technology, Generic decryption (GD) technology), Host-based Behavior-blocking software	3T + 3P
6.	Intrusion Detection Requirements of an IDS, Analysis Approaches: Anomaly Detection, Signature or Heuristic Detection, Host-Based Intrusion detection, Distributed IDS, Network IDS, Types of Network Sensors, Intrusion Detection Techniques in NIDS, Functional components of an IDS, Honeypots, SNORT IDS, Firewall, Need of Firewalls, Firewall characteristics and Access policy, Firewall limitations, VPN Self-Study Topic(s): Intrusion detection exchange Format, NIDS Sensor Deployment, Type of Firewalls, IPS, HIPS, NIPS	4T + 4P
Total		22T+22P

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm Exam	5th-6th week	15%
2.	Assignment I	7th week	10%
3.	Assignment II (Case Study/ Group assignment)	9th week	15%
4.	Lab Exam	11th Week	20%
5.	Final Theory Exam	12th Week	40%
...			

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	W. Stallings, Computer Security: Principles and Practice, Pearson, 4th Edition, 2019. ISBN-13 : 978-9353438869
Supportive References	• Elementary Information Security, Richard E. Smith, 2019, 3rd edition, Jones & Bartlet Learning, ISBN-13: 978-1284153040 • W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8th edition, 2019. ISBN-13: 978- 0135764183 • Computer Security: Art and Science, Matt Bishop, 2019, 2nd edition, Addison-Wesley Professional, ISBN-13: 978-0321712332
Electronic Materials	• https://learncryptography.com/ • https://www.garykessler.net/library/crypto.html • https://gpgtools.tenderapp.com/kb/how-to/introduction-to-cryptography • https://www.khanacademy.org/computing/computer-science/cryptography
Other Learning Materials	

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• Classroom equipped with projector, whiteboard, and sufficient seating arrangements. • Lab with software installed and an individual computer terminal for each student.

Items	Resources
Technology equipment (projector, smart board, software)	• Whiteboards and projectors for classroom and labs Following software for lab work: • Kali Linux
Other equipment (depending on the nature of the specialty)	None

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students	Indirect (Course evaluation survey form)
Effectiveness of students assessment	CRC / QAU / HoD	Direct (Course reports / result analysis)
Quality of learning resources	Track leaders / CRC	Indirect (Review, meetings and star rating with suggestions for further modification and improvements)
The extent to which CLOs have been achieved	CRC / QAU	Direct (CLO assessment template further verified at course coordinator, Track leader and QAU level)
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	DEPARTMENT COUNCIL
REFERENCE NO.	
DATE	15/10/2022