هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

2023
TP-153

Course Specification
(Bachelor)

Course Title:	Computer Security and Privacy
Course Code:	COMP-323
Program:	Bachelor in Computer Science
Department:	Computer Science
College:	College of Engineering and Computer Science
Institution:	Jazan University
Version:	V2
Last Revision Date:	07 January 2023

Table of Contents

A. General information about the course: 3

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods 4

C. Course Content 5

D. Students Assessment Activities 6

E. Learning Resources and Facilities 7

F. Assessment of Course Quality 7

G. Specification Approval 8

A. General information about the course:

1. Course Identification

1. Credit hours: (03)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		
3. Level/year at which this course is offered: (Level 06 / Year 03)					
4. Course General Description:					
This course provides integrated, comprehensive, and up-to-date coverage of Computer Security topics. The topics cover 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)**:**					
Nil					
6. Pre-requirements for this course (if any)**:**					
Nil					
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.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	60	100%

No	Mode of Instruction	Contact Hours	Percentage
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning (Self-Learning)		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	28
2.	**Laboratory/Studio**	28
3.	**Field**	--
4.	**Tutorial**	--
5.	**Others (specify)**	4
Total		60

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

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
2.2	**Justify** appropriate encryption standards and techniques to suit specific business and technological needs.	**S2**	• Lectures /Presentations • Media Lectures Tutorials	• Assignment - 1 • Assignment – 2 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** Chapter One: Overview Introduction, Definition of Computer Security, CIA triad, Challenges of Computer Security, Computer Security Terminology, Security Concepts and Relationships, System Assets, Vulnerabilities, Threats and Attacks, Types of Attacks, Countermeasures, Threat Consequences, Threat Actions, Network Security Attacks	4T + 4P
2.	**Cryptographic Tools** Symmetric encryption, Cryptanalysis, brute-force attack, Symmetric Block Encryption Algorithms: DES, Triple DES, AES Random and Pseudo-random numbers, Stream Cipher, Block vs Stream Ciphers, 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, Digital Envelopes, Digital Signature Standard, Elliptic-Curve Cryptography	6T + 6P
3.	**User Authentication**	4T + 4P

	Authentication process, Means of Authentication, Password-Based Authentication, Vulnerability of Passwords, Password Selection Strategies, Hashed Passwords, Password Cracking, Password Selection Strategies, Password File Access Control, Token-Based Authentication, Biometric Authentication, Physical Characteristics Used in Biometric Applications, Operation of a Biometric Authentication System, Security Issues for User Authentication, Defenses	
4.	**Access Control** Access Control, Access Control Context, Access Control Policies, Subjects, Objects, and Access Rights, Discretionary Access Control, Role-based Access Control, Attribute-based access control, ABAC Model Attributes Identity management, Credential management, Access management	4T + 4P
5.	**Malicious Software** Malware, Types of Malware, Nature of Viruses, Virus Components, Phases of Computer Virus Lifetime, Viruses Classification, Clickjacking, Keylogger, Bot and Botnet, Phishing and Identity Theft, Malware Countermeasure Approaches, Antivirus and Generations of Antivirus **Denial of Service** Denial-of-service (DoS) attack, Forms of DoS attack, Source Address Spoofing, SYN spoofing attack, Flooding attacks, Defenses against Denial-of-service attacks	4T + 4P
6.	**Intrusion Detection** Intruders, classes of intruders, examples of intrusion, Intruder Behavior, Intrusion Detection, logical components of IDS, Types of IDS, Distributed or hybrid IDS, False positive, False negatives, IDS Requirements, Analysis Approaches: Anomaly Detection, Signature or Heuristic Detection, Host-Based Intrusion Detection, Distributed IDS, Network IDS, Types of Network Sensors, Honeypots, SNORT IDS, Firewall, VPN, Intrusion Prevention Systems (IPS), Host-Based IPS, Network-Based IPS, Distributed or Hybrid IPS	4T + 4P
Total		**26T + 26P**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm Exam	7th-8th week	15%
2.	Assignment I	9th week	10%
3.	Assignment II (Case Study/ Group assignment)	12th week	15%
4.	Lab Exam	14th Week	20%
5.	Final Theory Exam	15th 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.
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)

Assessment Areas/Issues	Assessor	Assessment Methods
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		

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

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