Course Specification
(Bachelor)

Course Title:	Computer Security
Course Code:	563CCS-3
Program:	Bachelor of Science in Computer Science
Department:	Department of Computer Science
College:	Computer Science and Information Systems
Institution:	Najran University
Version:	2.0
Last Revision Date:	August 2022

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3)

3 (2, 2, 1) [Theory, Lab, Tutorial]

2. Course type

A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐Elective		

3. Level/year at which this course is offered: (Level 10/Year 5)

4. Course General Description:

Introduction to Computer security and its terminology, user authentication, and Security services: confidentiality, integrity, availability. Security flaws and vulnerabilities. Symmetric & Asymmetric cryptography tools such as DES, 3DES, and AES. Message authentication and protocols such as Hash function, SHA-3. Malicious software, Denial of service attacks, intrusion detection systems, firewalls, and intrusion prevention systems. Internet security protocols and applications.

5. Pre-requirements for this course (if any)**:**

461CCS-3 (Data Communication and Computer Networks)

6. Co-requisites for this course (if any)**:**

None

7. Course Main Objective(s):

1. Define the basic concepts and terminologies of computer security.
2. Describe types of attacks related to computer/network systems and security services.
3. Distinguish symmetric and asymmetric cryptographic algorithms and their applications.
4. Classify user and message authentication algorithms and their applications.
5. Evaluate different types of malicious software, intrusion detection and prevention methods.
6. Illustrate the security protocols & applications devised for the internet.

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	75	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	30
2.	**Laboratory/Studio**	30
3.	**Field**	
4.	**Tutorial**	15
5.	**Others (specify)**	
Total		75

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

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Define the basic concepts and terminologies of computer security.	K1	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam
1.2	Describe types of attacks related to computer/network systems and security services.	K2	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam
1.3	Illustrate the security protocols & applications devised for the internet. And distinguish between different firewalls.	K1 , K2	Lectures, Lab Demonstrations	Quiz 2, Mid Exam, Final Lab Exam, Final Exam
2.0	**Skills**			

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
2.1	Distinguish symmetric and asymmetric cryptographic algorithms and their applications.	S1, S4	Lectures, Lab Demonstrations, Group Discussions	Mid Exam, Final Lab Exam, Final Exam
2.2	Classify user and message authentication algorithms and their applications.	S3, S4	Lectures, Lab Demonstrations	Quiz 2, Mid Exam, Final Lab Exam, Final Exam
2.3	Evaluate different types of malicious software, intrusion detection and prevention methods.	S2, S4	Lectures, Lab Demonstrations	Mid Exam, Final Lab Exam, Final Exam
2.4				
3.0	**Values, autonomy, and responsibility**			
3.1				
3.2				

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction to computer security concepts	5
2.	Cryptographic Tools	10
3.	User Authentication	5
4.	Symmetric encryption & message confidentiality	10
5.	Public key cryptography	5
6.	Hash Algorithms	5
7.	Key management & distribution	10
8.	Malicious software	5
9.	Internet security protocols	5
10.	Internet authentication applications	5
11.	Intrusion detection	5
12.	Intrusion Prevention & Firewalls	5
Total		**75**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Quizzes	3rd and 6th week	10%
2.	Theory Assignment or mini project (presentation)	4th week	10%
3.	Lab Participation	Full Semester	5%
4.	Midterm Exam	7th week	20%
5.	Lab Assessment	3rd week	5%
6.	Final Lab Exam	14th week	10%
7.	Final Theory Exam	16th or 17th 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	William Stallings and Lawrie Brown, Computer Security Principles and Practice, Pearson/Prentice Hall, Latest Edition.
Supportive References	Stallings, W., Cryptography and Network Security: Principles and Practice, Prentice Hall
Electronic Materials	Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing, Prentice-Hall
Other Learning Materials	NA

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• Lecture Rooms with an appropriate number of seats, Projector with Screen and a whiteboard or a smart board. • All the computers in all the laboratories should be installed with the latest version of the required software.
Technology equipment (projector, smart board, software)	• One PC and one projector and data show in the lecture room • Number of PCs according to the strength of students in the lab room
Other equipment (depending on the nature of the specialty)	NetBeans Software + Kali Linux in Labs

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Collecting students' suggestions to facilitate more during the class.	Students	Verbal discussion
Student's questionnaire once during the semester about course learning outcomes.	Students	Indirect Survey
Achievement percentage of course learning outcomes, direct evaluation using CLO assessment sheet	Course Instructor	Direct evaluation using CLO achievement calculation
Teaching strategies	Quality unit	Indirect
Assessment methods	Quality unit	Indirect
Instructor performance	Quality unit	Indirect
Course content	Quality unit	Indirect

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	Computer Science Departmental Council
REFERENCE NO.	14440203-0185-00002
DATE	1st Sep, 2022