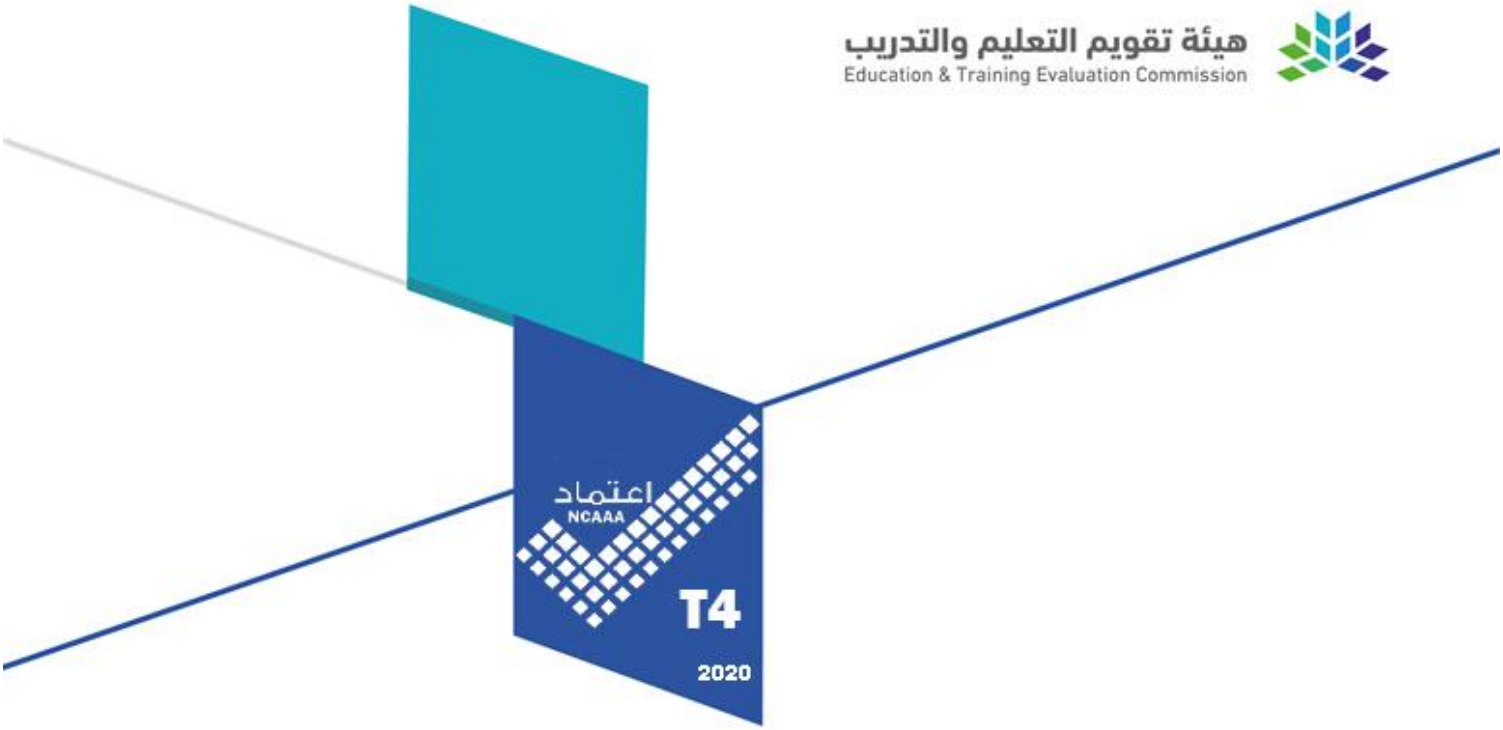
هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission



Course Specifications

Course Title:	Computer Security
Course Code:	563CCS-3
Program:	BSc in Computer Science
Department:	Department of Computer Science
College:	College of Computer Science and Information Systems
Institution:	Najran University

Table of Contents

A. Course Identification

1. Credit hours:
2. Course type **a.** University ☐ College ☐ Department ☑ Others ☐ **b.** Required ☑ Elective ☐
3. Level/year at which this course is offered: Year 5 / Level 13
4. Pre-requisites for this course (if any)**:** 329CSS-3 Data Communication and Computer Networks
5. Co-requisites for this course (if any)**:** **N/A**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	50	100%
2	**Blended**		
3	**E-learning**		
4	**Distance learning**		
5	**Other**		

7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	**Lecture**	20
2	**Laboratory/Studio**	20
3	**Tutorial**	10
4	**Others** (specify)	
	Total	**50**

B. Course Objectives and Learning Outcomes

1. Course Description

Introduction to Computer security and its terminology, user authentication, 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 system, firewalls, and intrusion prevention system. Internet security protocols and applications.

2. Course Main Objective

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 internet.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge and Understanding**	
1.1	Define the basic concepts and terminologies of computer security.	K_1
1.2	Describe types of attacks related to computer/network systems and security services.	K_2
1.3	Illustrate the security protocols & applications devised for internet.	K_1, K_2
1...		
2	**Skills :**	
2.1	Distinguish symmetric and asymmetric cryptographic algorithms and their applications.	S_1, S_4
2.2	Classify user and message authentication algorithms and their applications.	S3, S_4
2.3	Evaluate different types of malicious software, intrusion detection and prevention methods.	S_2, S_4
2.4		
3	**Values:**	
3.1		
3.2		
3.3		
3...		

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to computer security concepts	5
2	Cryptographic Tools	5
3	User Authentication	5
4	Symmetric encryption & message confidentiality	5
5	Public key cryptography	5
6	Hash Algorithms	5
7	Key management & distribution	5
8	Malicious software	5
9	Internet security protocols	5
10	Internet authentication applications	5
11	Intrusion detection	5
12	Intrusion prevention & Firewalls	5
Total		50

D. Teaching and Assessment

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
1.0	**Knowledge and Understanding**		
1.1	Define the basic concepts and terminologies of computer security.	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam
1.2	Describe types of attacks related to computer/network systems and security services.	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam
1.3	Illustrate the security protocols & applications devised for internet. And distinguish between different firewalls.	Lectures, Lab Demonstrations	Quiz 2, Mid Exam, Final Lab Exam, Final Exam
2.0	**Skills**		
2.1	Distinguish symmetric and asymmetric cryptographic algorithms and their applications.	Lectures, Lab Demonstrations, Group Discussions	Mid Exam, Final Lab Exam, Final Exam
2.2	Classify user and message authentication algorithms and their applications.	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.	Lectures, Lab Demonstrations	Mid Exam, Final Lab Exam, Final Exam
3.0	**Values**		
3.1			
3.2			
…			

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	Quizzes	2nd week	10%
2	Theory Assignment or mini project (presentation)	4th week	10%
3	Lab Participation	Full Semester	5%
4	Midterm Exam	6th week	20%
5	Lab Assessment	3rd week	5%
6	Final Lab Exam	11	10%
7	Final Theory Exam	12 or 13	40%
	Total		**100%**

***Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

E. Student Academic Counseling and Support

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :

- 10 weekly office hours + appointments

- 3 weekly academic advising hours
- Extra weekly 2 office hours prior to exams.

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	William Stallings and Lawrie Brown, **Computer Security Principles and Practice**, Pearson/Prentice Hall, Latest Edition.
Essential References Materials	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	N/A

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	• Lecture Rooms with appropriate number of seats, Projector with Screen and a white board or a smart board. • All the computers in all the laboratories should be installed with the latest version of the required software.
Technology Resources (AV, data show, Smart Board, software, etc.)	• One PC and one projector and data show in the lecture room • Number of PCs according to strength of students in the lab room
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	NetBeans Software + Kali Linux in Labs

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Collecting students' questionnaire about the faculty and teaching methods.	Students	Survey
Effectiveness of teaching and assessment	Students	Direct
Focus group discussion with small groups of students.	instructor	Direct
Extent of achievement of course learning outcomes	instructor	Direct
The quality of learning resources	Program Leaders	direct

Evaluation Areas/Issues	Evaluators	Evaluation Methods

Evaluation areas (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)
Evaluators (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
Assessment Methods (Direct, Indirect)

H. Specification Approval Data

Council / Committee	Computer Science Departmental Council
Reference No.	14440203-0185-00002
Date	1st Sep, 2022