Course Specifications

Course Title:	**Mobil Security**
Course Code:	**CSEC 416**
Program:	**Information and Computer Science**
Department:	**Computer Science and Information**
College:	**Science**
Institution:	**Majmaah University**

Table of Contents

A. Course Identification **3**

6. Mode of Instruction (mark all that apply) 3

B. Course Objectives and Learning Outcomes **4**

1. Course Description 4

2. Course Main Objective 4

3. Course Learning Outcomes 4

C. Course Content **4**

D. Teaching and Assessment **5**

1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods 5

2. Assessment Tasks for Students 5

E. Student Academic Counseling and Support **6**

F. Learning Resources and Facilities **6**

1.Learning Resources 6

2. Facilities Required 6

G. Course Quality Evaluation **7**

H. Specification Approval Data **7**

A. Course Identification

1. Credit hours:3
2. Course type **a.** University ☐ College ☐ Department ☐ Others ☐ **b.** Required ☐ Elective ☒
3. Level/year at which this course is offered: Selective
4. Pre-requisites for this course (if any)**:** ICS 322 & CSEC 323
5. Co-requisites for this course (if any)**:**

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**	48	80%
2	**Blended**	6	10%
3	**E-learning**	6	10%
4	**Correspondence**	0	0%
5	**Other**	0	0%

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	30
2	**Laboratory/Studio**	0
3	**Tutorial**	30
4	**Others** (specify)	0
	Total	60
Other Learning Hours*		
1	**Study**	45
2	**Assignments**	15
3	**Library**	10
4	**Projects/Research Essays/Theses**	10
5	**Others** (specify)	0
	Total	80

***** The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course provides a good conceptual overview of the security principles incorporated in the design of several generations of mobile networks, from GSM (2G), UMTS (3G) up until LTE (4G). We also explore platform security models of the popular mobile device platforms including IOS, Android and the Windows Phone. This course also covers the security of mobile services, such as VoIP, text messaging, WAP and mobile HTML.

2. Course Main Objective

1. Understand fundamental mobile computing principles and models and mobile
2. computing security principles.
3. Understand the fundamental elements and role of encryption in mobile application and device security, and describe common scenarios where encryption processes
4. Understand common threats and vulnerabilities related to mobile computing networks, and explain the concepts of defending against and managing network
5. Understand mobile computing physical access control models, and describe common approaches to control access to the physical resources of an organization

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	Explain the vulnerabilities introduced into an infrastructure by wireless and cellular technologies.	K3-CS
1.2	Recommend security hardening techniques for wireless or mobile technologies.	K3-CS
2	**Skills :**	
2.1	Recommend security hardening techniques for wireless or mobile technologies.	S3-CS
2.2	Compare and contrast the needs of law-enforcement versus individual right-to-privacy in wireless infrastructures.	S3-CS
3	**Competence:**	
3.1	Prepare a group presentation or individual written assignment on a relevant wireless or mobile security topic.	C3-CS
3.2	Produce a relevant wireless or mobile security team project.	C3-CS

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to Mobile Security	4
2	Building Blocks – Basic security and cryptographic techniques.	8
3	Security of GSM Networks	4
4	Security of UMTS Networks	4
5	LTE Security	4
6	WiFi and Bluetooth Security	4
7	SIM/UICC Security	4
8	Mobile Malware and App Security	4
9	Android Security Model	4
10	IOS Security Model	4
11	Security Model of the Windows Phone	4

12	SMS/MMS, Mobile Geolocation and Mobile Web Security.	4
13	Security of Mobile VoIP Communications	4
14	Emerging Trends in Mobile Security	4
Total		60

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**		
1.1	Explain the vulnerabilities introduced into an infrastructure by wireless and cellular technologies.	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Recommend security hardening techniques for wireless or mobile technologies.		
2.0	**Skills :**		
2.1	Recommend security hardening techniques for wireless or mobile technologies.	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	Compare and contrast the needs of law-enforcement versus individual right-to-privacy in wireless infrastructures.		
3.0	**Competence:**		
3.1	Prepare a group presentation or individual written assignment on a relevant wireless or mobile security topic.	Small group discussion Whole group discussion Brainstorming Presentation	Observations Homework assignments Lab assignments Class Activities
3.2	Produce a relevant wireless or mobile security team project.		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented algorithms	Every two weeks	10%
6	Final written exam	16	40%
7	Total		100%
8			

***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 :

Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

- 6-office hours per week in the lecturer schedule.
- The contact with students by e-mail, mobile, office telephone, website and Black Board

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	Mobile Application Security 1st Edition by Himanshu Dwivedi, Chris Clark, and David Thiel, Himanshu Dwivedi, ISBN-13: 978-0071633567, 2020.
Essential References Materials	Wireless and Mobile Device Security: Print Bundle (Jones & Barlett Learning Information Systems Security & Assurance) Illustrated Edition, Kindle Edition by Jim Doherty (Author)
Electronic Materials	Video lectures are available for students at the time of the course.
Other Learning Materials	https://solutionsreview.com/mobile-device-management/the-top-8-mobile-security-books-you-need-to-read/

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classroom and Labe available at College of science in Zulfi.
Technology Resources (AV, data show, Smart Board, software, etc.)	All resource are available in the halls
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	N\A

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Effectiveness of teaching and assessment	Students Reviewers	Questionnaires (course evaluation) filled by the students and electronically organized by the university. Student-faculty and management meetings.
Quality of learning resources	Program Leaders	Direct/indirect

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	
Reference No.	
Date	