



## Course Specifications

<b>Course Title:</b>	<b>Network Security</b>
<b>Course Code:</b>	<b>CSI 432</b>
<b>Program:</b>	<b>Computer Science and Information Technologies</b>
<b>Department:</b>	<b>Computer Science and Information</b>
<b>College:</b>	<b>College of Science at Al Zulfi</b>
<b>Institution:</b>	<b>Majmaah University</b>

## Table of Contents

<b>A. Course Identification</b> .....	<b>3</b>
6. Mode of Instruction (mark all that apply) .....	3
<b>B. Course Objectives and Learning Outcomes</b> .....	<b>3</b>
1. Course Description .....	3
2. Course Main Objective.....	3
3. Course Learning Outcomes .....	4
<b>C. Course Content</b> .....	<b>4</b>
<b>D. Teaching and Assessment</b> .....	<b>5</b>
1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods .....	5
2. Assessment Tasks for Students .....	6
<b>E. Student Academic Counseling and Support</b> .....	<b>6</b>
<b>F. Learning Resources and Facilities</b> .....	<b>6</b>
1. Learning Resources .....	6
2. Facilities Required.....	7
<b>G. Course Quality Evaluation</b> .....	<b>7</b>
<b>H. Specification Approval Data</b> .....	<b>7</b>

## A. Course Identification

<b>1. Credit hours:</b>
<b>2. Course type</b>
a. University <input type="checkbox"/> College <input type="checkbox"/> Department <input checked="" type="checkbox"/> Others <input type="checkbox"/>
b. Required <input type="checkbox"/> Elective <input checked="" type="checkbox"/>
<b>3. Level/year at which this course is offered:</b> 7 <sup>th</sup> level
<b>4. Pre-requisites for this course (if any):</b>
Advanced Computer Networks (CSI 431)
<b>5. Co-requisites for this course (if any):</b>
N/A

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

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom		80%
2	Blended		10%
3	E-learning		10%
4	Distance learning		-
5	Other		-

### 7. Contact Hours (based on academic semester)

No	Activity	Contact Hours
1	Lecture	30
2	Laboratory/Studio	30
3	Tutorial	-
4	Others (specify)	-
	<b>Total</b>	<b>60</b>

## B. Course Objectives and Learning Outcomes

<p><b>1. Course Description</b></p> <p>This course provides an introduction to the field of network security. Specific topics to be examined include security attacks, mechanisms, and services, network security, access security models, network security practice, Email security, IP security, web security, Intrusion detection, prevention systems, firewalls and virtual private networks, cellular and wireless network security</p>
<p><b>2. Course Main Objective</b></p> <p>This module aims :</p> <ol style="list-style-type: none"> <li>1. To introduce students with the importance of security for computer systems.</li> <li>2. To describe the security goals and the services of security system.</li> <li>3. To explain available methods of defense.</li> <li>4. To distinguish among Transport-Levels Security such as, Web Security Issues, Secure Sockets Layer (SSL) and Transport Layer Security (TLS).</li> </ol>



5. To understand Wireless Network Security and explains the general idea of, IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Wireless Application, Protocol Overview, Wireless Transport Layer Security and WAP End-to-End Security.

### 3. Course Learning Outcomes

CLOs		Aligned PLOs
<b>1</b>	<b>Knowledge and Understanding</b>	
1.1	Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of secure networking systems, and its underpinning science and mathematics;	K1
1.2	Asses the threats, vulnerabilities, and risks to a computer network.	K1
1.3	Identify the standards of security protocols for Emails, web security, and IP security.	K2
<b>2</b>	<b>Skills :</b>	
2.1	Demonstrate creative and innovative ability in the synthesis of solutions and in formulating designs in secure computer network systems;	S4
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems.	S4
<b>3</b>	<b>Values:</b>	
3.1	Work in a group and learn time management	C1
3.2	Learn how to search for information through library and internet.	C1
3.3	Present a short report in a written form and orally using appropriate scientific language	C1

### C. Course Content

No	List of Topics	Contact Hours
1	Introduction .The importance of network security	4
2	Key Distribution and User Authentication <ul style="list-style-type: none"> <li>• Symmetric Key Distribution Using Symmetric Encryption</li> <li>• Kerberos</li> <li>• Key Distribution Using Asymmetric Encryption</li> <li>• X.509 Certificates</li> <li>• Public Key Infrastructure</li> <li>• Federated Identity Management</li> </ul>	12
3	Transport-Level Security <ul style="list-style-type: none"> <li>• Web Security Issues</li> <li>• Secure Sockets Layer (SSL)</li> <li>• Transport Layer Security (TLS)</li> <li>• HTTPS</li> </ul>	12



	<ul style="list-style-type: none"> <li>Secure Shell (SSH)</li> </ul>	
4	<b>Wireless Network Security</b> <ul style="list-style-type: none"> <li>IEEE 802.11 Wireless LAN Overview</li> <li>IEEE 802.11i Wireless LAN Security</li> <li>Wireless Application Protocol Overview</li> <li>Wireless Transport Layer Security</li> <li>WAP End-to-End Security</li> </ul>	12
5	<b>IP Security</b> <ul style="list-style-type: none"> <li>IP Security Overview</li> <li>IP Security Policy</li> <li>Encapsulating Security Payload</li> <li>Combining Security Associations</li> <li>Internet Key Exchange</li> <li>Cryptographic Suites</li> </ul>	12
6	<b>Email Security</b> <ul style="list-style-type: none"> <li>PGP</li> <li>S/MIME</li> <li>Domain Keys Identifications Mail</li> </ul>	8
<b>Total</b>		

## 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	<b>Knowledge and Understanding</b>		
1.1	Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of secure networking systems, and its underpinning science and mathematics;	Lectures. Lab demonstrations. Case studies. Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Asses the threats, vulnerabilities, and risks to a computer network.		
1.3	Identify the standards of security protocols for Emails, web security, and IP security.		
2.0	<b>Skills</b>		
2.1	Demonstrate creative and innovative ability in the synthesis of solutions and	Lectures. Lab demonstrations.	Written Exam

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
	in formulating designs in secure computer network systems;	Case studies. Individual presentations.	Homework assignments Lab assignments
2.2	Apply relevant analytical and modeling techniques for specification and design of security based systems.	Brainstorming.	Class Activities Quizzes Observations
<b>3.0</b>	<b>Values</b>		
3.1	Set up, test and administer security systems for effective use;	Small group discussions. Whole group discussions.	Observations Homework assignments
3.2	Make effective oral presentations, both formally and informally	Brainstorming. Presentations.	Lab assignments Class Activities

## 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 protocols	Every two weeks	10%
6	Final written exam	16	40%

\*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 :**

1. A total of 6 office hours per week in the lecturer schedule in order to facilitate the student.
2. Contacting students using e-mail , mobile, office telephone and website

## F. Learning Resources and Facilities

### 1. Learning Resources

<b>Required Textbooks</b>	Czarnul, P. (2018). Parallel Programming for Modern High Performance Computing Systems. Chapman and Hall/CRC.
<b>Essential References Materials</b>	<ul style="list-style-type: none"> <li>• Douglas Jacobson, Introduction to Network Security, Taylor &amp; Francis, 2008.</li> <li>W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013.</li> </ul>

<b>Electronic Materials</b>	www.iacr.org
<b>Other Learning Materials</b>	N/A

## 2. Facilities Required

Item	Resources
<b>Accommodation</b> (Classrooms, laboratories, demonstration rooms/labs, etc.)	Classrooms and Labs as that available at college of science at Az-Zulfi are enough.
<b>Technology Resources</b> (AV, data show, Smart Board, software, etc.)	Smart Board
<b>Other Resources</b> (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	Students	<ul style="list-style-type: none"> <li>Analysis of students' results. Observation during class work.</li> <li>Students' evaluations.</li> <li>Colleagues' evaluations.</li> <li>Evaluation questionnaire filled by the students.</li> </ul> Interview a sample of students enrolled in the course to take their opinions
Evaluation of Teaching	Program leaders	<ul style="list-style-type: none"> <li>Self-assessment.</li> <li>External evaluation.</li> </ul> Periodic review of course (the Commission of study plans)

**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

<b>Council / Committee</b>	
<b>Reference No.</b>	
<b>Date</b>	

