



# **COURSE SPECIFICATIONS (CS)**

## Course Specifications

Institution: Najran University	Date: August 2017
College/Department : College of Computer Science and Information Systems/ Department of Computer Science	

### A. Course Identification and General Information

1. Course title and code: <b>Computer Security 429CSS-3</b>			
2. Credit hours: 3			
3. Program(s) in which the course is offered. <b>Bachelor of Science in Computer Science</b> (If general elective available in many programs indicate this rather than list programs)			
4. Name of faculty member responsible for the course: <b>Nyla Khadam</b>			
5. Level/year at which this course is offered: <b>Level 9</b>			
6. Pre-requisites for this course (if any): <b>329CSS-3 Data Communication and Computer Networks</b>			
7. Co-requisites for this course (if any): N/A			
8. Location if not on main campus: <b>Female Campus</b>			
9. Mode of Instruction (mark all that apply):			
a. Traditional classroom	<input type="checkbox"/>	What percentage?	<input type="checkbox"/>
b. Blended (traditional and online)	<input checked="" type="checkbox"/>	What percentage?	<input type="text" value="100%"/>
c. E-learning	<input type="checkbox"/>	What percentage?	<input type="checkbox"/>
d. Correspondence	<input type="checkbox"/>	What percentage?	<input type="checkbox"/>
f. other	<input type="checkbox"/>	What percentage?	<input type="checkbox"/>
Comments:			

## B Objectives

1. What is the main purpose for this course?

After successful completion of this course students should be able to:

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.

2. Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)

- The course content should be consistent with the changing trends and technologies in the field of Computer Science.
- Hard copies and soft copies of the text books and reference books are provided to the students.
- Open Labs are assigned so that the students can avail extra time to solve their lab assignments and exercises.
- Question & Answers sessions during the lecture hour to inculcate students' participation towards active learning.

## C. Course Description (Note: General description in the form used in Bulletin or handbook)

### 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.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction to computer security concepts	1	4
Cryptographic Tools	1	5
User Authentication	1	4
Symmetric encryption & message confidentiality	2	5
Public key cryptography	1	4
Hash Algorithms	1	5
Key management & distribution	1	4
Malicious software	1	5
Internet security protocols	1	4
Internet authentication applications	1	4
Intrusion detection & prevention	2	10
Firewalls	2	10

2. Course components (total contact hours and credits per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other:	Total
Contact Hours	Planned	30	6	N/A	30		66
	Actual	30	6	N/A	30		66
Credit	Planned	2	0	1		0	3
	Actual	2	0	1		0	3

3. Additional private study/learning hours expected for students per week.

5-10

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategy

**On the table below are the five NQF Learning Domains, numbered in the left column.**

**First**, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and intended learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy ought to reasonably fit and flow together as an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	Knowledge		

1.1	CLO-1: Identify factors driving the need for network security and classify different types of attacks (DOS attacks) and identify their point of vulnerability in networks.	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam 1
1.2	CLO_3: Describe the mechanisms for security key distributions & management and differentiate between the authentication algorithms (digital signatures, MAC, Hash Algorithm, MD5, and SHA) and should also recognize applications of these algorithms.	Interactive Lectures, Group Discussions	Quiz 1, Mid Exam 1
1.3	CLO_4: Illustrate the security protocols & applications devised for internet. And distinguish between different firewalls.	Lectures, Lab Demonstrations	Quiz 2, Mid Exam 2, Final Lab Exam, Final Exam
<b>2.0</b>	<b>Cognitive Skills</b>		
2.1	CLO_2: Analyze & Apply cryptographic theories, principles & techniques that are used to establish security properties. (Symmetric & Asymmetric encryption: block ciphers, DES, AES, Triple DES, RC5, Public Key Cryptosystems, RSA)	Lectures, Lab Demonstrations, Group Discussions	Mid Exam 1, Final Lab Exam, Final Exam
2.2	CLO_3: Describe the mechanisms for security key distributions & management and differentiate between the authentication algorithms (digital signatures, MAC, Hash Algorithm, MD5, and SHA) and should also recognize applications of these algorithms.	Lectures, Lab Demonstrations	Quiz 2, Mid Exam 2, Final Lab Exam, Final Exam
2.3	CLO_5: Compare & contrast different types of malicious software, intruders and intrusion detection methods.	Lectures, Lab Demonstrations	Final Lab Exam, Final Exam
<b>3.0</b>	<b>Interpersonal Skills &amp; Responsibility</b>		
3.1	N/A		
3.2			
<b>4.0</b>	<b>Communication, Information Technology, Numerical</b>		
4.1	CLO_2: Analyze & Apply cryptographic theories, principles & techniques that are used to establish security properties. (Symmetric &	Lectures, Lab Demonstrations, Group Discussions	Mid Exam 1, Final Lab Exam, Final Exam

	Asymmetric encryption: block ciphers, DES, AES, Triple DES, RC5, Public Key Cryptosystems, RSA)		
4.2	CLO_3: Describe the mechanisms for security key distributions & management and differentiate between the authentication algorithms (digital signatures, MAC, Hash Algorithm, MD5, and SHA) and should also recognize applications of these algorithms.	Lectures, Lab Demonstrations	Quiz 2, Mid Exam 2, Final Lab Exam, Final Exam
4.3	CLO_4: Illustrate the security protocols & applications devised for internet. And distinguish between different firewalls.	Lectures, Group Discussions	Final Exam
<b>5.0</b>	<b>Psychomotor</b>		
5.1	N/A		
5.2			

5. Schedule of Assessment Tasks for Students During the Semester			
	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Quiz1	3 <sup>rd</sup> week	2%
2	Theory Assignment 1	5 <sup>th</sup> week	2%
3	Lab Participation	Full Semester	2%
4	Midterm Exam-I	6 <sup>th</sup> week	15%
5	Lab Assessment 1	7 <sup>th</sup> week	5%
6	Quiz 2	8 <sup>th</sup> week	2%
7	Lab Assessment 2	9 <sup>th</sup> week	3%
8	Theory Assignment 2	9 <sup>th</sup> week	2%
9	Midterm Exam-II	10 <sup>th</sup> week	15%
10	Theory Assignment 3	11 <sup>th</sup> week	2%
11	Final Lab Exam		10%
12	Final Theory Exam		40%
	<b>Total</b>		<b>100%</b>

## D. Student Academic Counseling and Support

1. 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)

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

## E Learning Resources

1. List Required Textbooks

- William Stallings and Lawrie Brown, **Computer Security Principles and Practice**, Pearson/Prentice Hall, Latest Edition.

2. List Essential References Materials (Journals, Reports, etc.)

- Stallings, W., **Cryptography and Network Security: Principles and Practice**, Prentice Hall

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

- Charles P. Pfleeger and Shari L. Pfleeger, **Security in Computing**, Prentice-Hall

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

- NetBeans for Lab Programs.

## F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
<p>1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)</p> <ul style="list-style-type: none"> <li>Lecture Rooms with appropriate number of seats, Projector with Screen and a white board or a smart board.</li> <li>All the computers in all the laboratories should be installed with the latest version of the required software.</li> </ul>
<p>2. Technology resources (AV, data show, Smart Board, software, etc.)</p> <ul style="list-style-type: none"> <li>One PC and one projector and data show in the lecture room</li> <li>Number of PCs according to strength of students in the lab room</li> </ul>
<p>3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)</p> <ul style="list-style-type: none"> <li>NetBeans Software in Labs</li> </ul>

## G Course Evaluation and Improvement Processes

<p>1. Strategies for Obtaining Student Feedback on Effectiveness of Teaching</p> <ul style="list-style-type: none"> <li>Online Course Survey: By the end of each semester, students give their opinions about many factors in the course. They give feedback about the teaching strategies, assessment methods, textbooks, instructor, etc.</li> <li>Feedback about Course Learning Outcomes (CLOs): A course survey is distributed to students to take their opinions about the CLOs.</li> </ul>
<p>2. Other Strategies for Evaluation of Teaching by the Instructor or by the Department</p> <ul style="list-style-type: none"> <li>Consulting peers on teaching.</li> <li>Discussion about the course in department.</li> <li>Discussion with experienced teaching staff in the subject.</li> <li>Using e-mails to receive students' expectation in the course.</li> </ul>
<p>3. Processes for Improvement of Teaching</p> <ul style="list-style-type: none"> <li>Relate CLOs to assessment methods and teaching strategies</li> <li>Describe the relationships between the course's topics and CLOs.</li> <li>Course syllabus must be distributed in the first week. It should contain the necessary information about the course (CLOs, assessment methods, descriptions, etc.)</li> <li>Implement the improvement plan of previous semester.</li> <li>Ensure that all students participate in the class.</li> <li>Encourage students to attend tutorials and to benefit from office hours.</li> <li>Contact lab instructor to make sure that the theory is consistent with the lab materials.</li> </ul>




4. Processes for Verifying Standards of Student Achievement (e.g. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution)

- Mid and Final exams are reviewed by Course Coordinators to check the compatibility between questions and CLOs.
- All the exams (mid and final ) and final grade sheet will be rechecked by a faculty member assigned by GEC before the final result.
- Vice Dean and Dean will review and approve the final grades before publishing on the internet.

5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.

- Each instructor has to teach the course according to the previous course materials and improvement plans.
- By the end of each semester, a course file containing all activities and samples must be prepared and submitted to the college.
- Evaluation of CLOs can be used to compare the improvement from previous evaluation.
- Improvement plan based on the online course survey must be prepared.
- Action plan based on the CLOs achievements must be prepared.

Name of Course Instructor: **Nyla Khadam**

Signature: 

Date Specification Completed: **August 2017**

Program Coordinator: **Dr. Abdulrahman Thaqfan**

Signature:  \_

Date Received: \_\_\_\_\_