Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكــة العربيــة السعوديــة
الهيئــة الوطنيــة للتقويــم
والاعـتـمــاد الأكـاديـمــي

ATTACHMENT 5.

Kingdom of Saudi Arabia

The National Commission for Academic Accreditation & Assessment

14013602-3 Computer Security

T6. Course Specifications
(CS)

المملكــة العربيــة السعوديــة
الهيئــة الوطنيــة للتقويــم
والاعــتـمــاد الأكـاديـمــي

Course Specifications

Institution Umm Al Qura University	Date 15/4/2016

College/Department College of Computers and Information Systems/ Computer Science Department

A. Course Identification and General Information

1. Course title and code: 14013602-3 Computer Security
2. Credit hours: 3
3. Program(s) in which the course is offered. (If general elective available in many programs indicate this rather than list programs)
4. Name of faculty member responsible for the course Sultan Almotiri
5. Level/year at which this course is offered 3rd Year Level 8
6. Pre-requisites for this course (if any) 14012601-4 Computer Networks.
7. Co-requisites for this course (if any)
8. Location if not on main campus : Al-Abidiyah campus (Boys) and Al-Zaher campus (Girls), Makkah Al Mukarramah
9. Mode of Instruction (mark all that apply)

a. traditional classroom	✓	What percentage?	80%
b. blended (traditional and online)		What percentage?	
c. e-learning	✓	What percentage?	20%
d. correspondence		What percentage?	
f. other		What percentage?	

Comments:

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكــة العربيــة السعوديــة
الهيئـــة الوطنيـــة للتقويـــم
والاعـتـمــاد الأكــاديـمــي

B Objectives

1. What is the main purpose for this course?

This course is the first level of computer and network security. The course will cover various topics related to computer security, data privacy, network protection against various attacks. The course gives students enough knowledge and a reasonable background to understand network security, active and passive attacks, Internet privacy, secure communications. Students are expected to practice biweekly homeworks, develop critical thinking about computer and network security, and apply learned materials in different contexts of various attacks, wireless and Internet security.

1. State the basic concepts in information security, including security policies, security models, and security mechanisms.
2. Explain concepts related to applied cryptography, including plain-text, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
3. Explain the concepts of malicious code, including virus, Trojan horse, and worms
4. Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation
5. Outline the requirements and mechanisms for identification and authentication
6. Explain issues about password authentication, including dictionary attacks (password guessing attacks), password management policies, and one-time password mechanisms
7. Explain the requirements for trusted operating systems, and describe the independent evaluation, including evaluation criteria and evaluation process
8. Describe security requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases
9. Describe threats to networks, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection
10. Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls

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)

This Course is one of the frequently revised courses by committee of study's scheduling and planning to ensure its follow-up to the up-to-date development major, from the following aspects:
1- Using up-to-date topic-related references
2- Revising scientific achievements that are related to course field.
3- Keeping track of activities for Associates and companies that are interested in course field.
4- Following-up outcomes from related scientific researches.
5- Attending Scientific conferences

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

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكــة العربيــة السعوديــة
الهيئــة الوطنيــة للتقويــم
والاعـتـمـاد الأكـاديـمــي

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
1. Introduction Basic Concepts: Threats, Vulnerabilities, Controls; risk; confidentiality, integrity, availability, security policies, security mechanisms, assurance; prevention, detection, deterrence	1	3
2. Basic cryptography Basic cryptographic terms, Historical background, Symmetric crypto primitives, Modes of operation, Cryptographic hash functions, Asymmetric crypto primitives	2	4
3. Program security Flaws: Malicious code: viruses, Trojan horses, worms; Program flaws: buffer overflows, time-of-check to time-of-use flaws, incomplete mediation, Defenses: Software development controls, Testing techniques	2	4
4. Operating Systems Security Operating Systems Concepts, Operating Systems Security, File System Access Control, Buffer Overflow Attacks	2	6
5. Database management systems security Database integrity, Database secrecy, Inference control, Multilevel databases	2	4
6. Network security Network threats: eavesdropping, spoofing, modification, denial of service attacks, Introduction to network security techniques: firewalls, virtual private networks, intrusion detection,	2	4
7. Web security Basic web security model, Web application security , Session management and user authentication, HTTPS: goals and pitfalls	2	4

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكـة العربيـة السعوديـة
الهيئــة الوطنيــة للتقويـم
والاعـتـمـاد الأكـاديـمـي

8. **Management of security** Security policies, Risk analysis, Physical threats and controls	1	3
9. **Miscellaneous** Legal aspects of security, Privacy and ethics	1	3

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

	Lecture	Tutorial	Laboratory or Studio	Practical	Other:	Total
Contact Hours	35	0	10	0	2 office hour per week	75
Credit	35	0	10	0	2 office hour per week	75

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

3

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	Appreciate the need for computer security and computer protection, including the tradeoffs between different security and protection methods	lectures, e-learning, assignments	*Quizzes, Assignments, Midterm Exam, Final Exam*
1.2	Able to apply concepts of public keys, private keys, cryptosystem, authentication, digital signatures to secure simple systems.	lectures, e-learning, assignments	Quizzes, Assignments, Midterm Exam, Final Exam

T6._Course Specifications_1 Feb 2015

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكـة العربيـة السعوديـة
الهيئـة الوطنيـة للتقويـم
والاعـتـمـاد الأكـاديـمـي

1.3	Implement some network security protocols such as SSL, MAC, and wireless security, WEP, WAP, and computer viruses, and Internet attacks, and utilize them in real applications to secure Internet traffic.	lectures, e-learning, assignments	Quizzes, Assignments, Midterm Exam, Final Exam
2.0	**Cognitive Skills**		
2.1	To enhance the students core ability to learn faster easier and better for new technology	lectures, e-learning, assignments	Quizzes, Assignments, Midterm Exam, Final Exam
2.2	<u>Will acquire the ability to understand</u> the threats and how to secure it	lectures, e-learning, assignments	Quizzes, Assignments, Midterm Exam, Final Exam
3.0	**Interpersonal Skills & Responsibility**		
3.1	Self-Learning which will help students manufacture their own body of knowledge by allowing them to experience learning through task based activities		
3.2			
4.0	**Communication, Information Technology, Numerical**		
4.1	Not applicable		
4.2			
5.0	**Psychomotor**		
5.1	Not applicable		
5.2			

 5. Map course LOs with the program LOs. (Place course LO #s in the left column and program LO #s across the top.)

Course LOs #	Program Learning Outcomes (Use Program LO Code #s provided in the Program Specifications)											
	1.1	**1.2**	**1.3**	**1.4**	**2.1**	**2.2**	**2.3**	**3.1**	**3.2**	**4.1**	**4.2**	**5.1**
1.1	I			I		I			I			
1.2	I											
1.3	I			I		I						

6. Schedule of Assessment Tasks for Students During the Semester

	Assessment task (e.g. essay, test, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Attendance and class participation	1-15	5%
2	Quiz 1	2	2.5%

T6._Course Specifications_1 Feb 2015

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكـة العربيـة السعوديـة
الهيئـة الوطنيـة للتقويـم
والاعـتـمـاد الأكـاديـمـي

3	Assignment 1	3	5%
4	Quiz 2	4	2.5%
5	Assignment 2	6	5%
6	Midterm	8	25%
7	Quiz 3	9	5%
8	Assignment 3	11	5%
9	Quiz 4	12	5%
10	Final exam	16	40%

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)
Every class is assigned 2 office hours per week..

E Learning Resources

1. List Required Textbooks
- Introduction to Computer Security, Michael T. Goodrich and Roberto Tamassia , Addison Wesley. 2011
- Charles P. Pfleeger and Shari L. Pfleeger. Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

2. List Essential References Materials (Journals, Reports, etc.)
Stallings, William, and Lawrie Brown. "Computer security." *Principles and Practice* (2008).

3. List Recommended Textbooks and Reference Material (Journals, Reports, etc)
 Russell, Deborah, and G. T. Gangemi. *Computer security basics*. " O'Reilly Media, Inc.", 1991.
Matt, Bishop. *Introduction to computer security*. Pearson Education India, 2006.

4. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
M. Bishop, "What is computer security?," in *IEEE Security & Privacy*, vol. 1, no. 1, pp. 67-69, Jan.-Feb. 2003.

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

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكــة العربيــة السعوديــة
الـهيئــة الوطنيــة للتقويــم
والاعـتـمــاد الأكــاديــمــي

Not Applicable

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.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) Lecture room (max 40 students) Computer lab (max 20 students)
2. Computing resources (AV, data show, Smart Board, software, etc.) Data Show, Smart board,
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list) Firewall devices,

G   Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching A student-feedback form is distributed at the end of the course.
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department University Course and Instructor Survey
3 Processes for Improvement of Teaching Review of curriculum and course. Coordination of instructors to improve the teaching quality.
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) Course file review
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.

Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكــة العربيــة السعوديــة
الهيئــة الوطنيــة للتقويــم
والاعــتــمــاد الأكـاديــمــي

> There are curriculum committee and Quality Assurance committee to review the course effectiveness.

Name of Instructor: Dr. Sultan Almotiri

Signature: Dr. Sultan Almotiri   Date Report Completed: 17th April 2016

Name of Course Instructor Dr. Sultan Almotiri

Program Coordinator:_____

Signature: _____   Date Received: _____