هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

2023
TP-153

Course Specification
(Bachelor)

Course Title:	Systems and Software Security
Course Code:	CENX 471
Program:	B.S. in Computer Engineering
Department:	Department of Computer Engineering
College:	College of Computer and Information Sciences
Institution:	King Saud University
Version:	1
Last Revision Date:	1444/2/5

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours: (3 hours)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☐ Required		☒ Elective		
3. Level/year at which this course is offered: (Level 9 and 10)					
4. Course general Description:					
Review of sampling theorem, filtering, and noise management; speech and language fundamentals; speech perception and production; tools for digitally processing speech signal: windowing, pre-emphasis, and framing; linear predictive coding; applications of digital speech processing such as speech recognition and synthesis.					
5. Pre-requirements for this course (if any)**:**					
Computer Networks, CENX 441					
6. Co-requirements for this course (if any)**:**					
7. Course Main Objective(s):					
Fundamental security concepts and terminology; Review of computer system components and the compilation life cycle; Introduction/review of Linux basics, assembly/debugging review; Reverse engineering overview; Malicious software (Malware, viruses, trojan horse, etc.); Software attacks: Control-flow hijacking and buffer overflow, code injection attacks, code reuse, command injection; Access control: access control policies and models, administration (e.g., privilege separation), attacks and vulnerabilities (e.g., privilege escalation, confused deputy); Advanced System and Software defenses (all or partial list of the following): Stack canaries, Data Execution Prevention, Address Space Layout Randomization, Trusted Computing; Applied Authentication Techniques and Protocols; Introduction to Password Cracking; Advanced Topics (e.g. IoT Security).					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	4 hours per week	100%
2	E-learning		
3	Hybrid • Traditional classroom • E-learning		
4	Distance learning		

3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	15
5.	**Others (specify)**	
Total		60

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Identify the main components of computer systems and software security.	**1 and 6**		
1.2	Understand and analyze authentication concepts, techniques, and attacks.	**2 and 6**		
2.0	**Skills**			
2.1	Demonstrate the exploit techniques used against vulnerable systems and software.	**4 and 5**		
2.2	Understand and discuss the implementation of computer systems and software security defenses and their limitations.	**3 and 6**		
3.0	**Values, autonomy, and responsibility**			
3.1	Apply exploit techniques and defenses on computer and software systems.	**2 and 7**		

C. Course Content

No	List of Topics	Contact Hours
1.	Introduction (security concepts and terminology), Lab and project set up	4
2.	Review of the compilation life cycle; Introduction/review of Linux basics, assembly/debugging review, Reverse Engineering	10
3.	Software attacks: Control-flow hijacking and buffer overflow, code injection attacks, code reuse, command injection	12
4.	System and Software defenses: Stack canaries, Data Execution Prevention, Address Space Layout Randomization	12
5.	Malicious software (Malware, viruses, trojan horse..etc.)	4
6.	Access Control	10
7.	Applied Authentication Techniques and Protocols; Introduction to Password Cracking	8
Total		60

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm Examination (1)	6	15%
2.	Midterm Examination (2)	12	15%
3.	Assignments and Quizzes	Bi-weekly	20%
4.	Project	Week 3 and week 10	10%
5.	Final Exam	End	40%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	• Software Security: Principles, Policies, and Protection, HexHive Books, July 2021. [Online]. Available: http://nebelwelt.net/SS3P/ • Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 3rd Edition, 2020.
Supportive References	
Electronic Materials	https://lms.ksu.edu.sa
Other Learning Materials	• Cryptography and Network Security: Principles and Practice, by William Stallings, 7th Edition, Prentice Hall, 2015. • Cryptography and Network Security, Behrouz A. Forouzan, McGraw Hill.

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Lecture room with number of seats enough to accommodate enrolled students.
Technology equipment (projector, smart board, software)	Overhead projector with required software to facilitate presentations on smart board.
Other equipment (depending on the nature of the specialty)	

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Department Council	Course reports are evaluated by the Department Council.
Effectiveness of Students assessment	Faculty-Peer Review	Final examination is moderated.
Quality of learning resources	Students	Indirect – Edu-gate survey.
The extent to which CLOs have been achieved	Students	Attainment level of every CLO is measured directly.
Other		

Assessors (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	