2023
TP-153

Course Specification
(Bachelor)

Course Title	**Computer and Information Security**
Course Code:	**CIT 1402**
Program:	**Bachelor in Information Technology**
Department:	**Department of Information Technology**
College:	**Faculty of Computers and Information Technology**
Institution:	**University of Tabuk**
Version:	**1.0**
Last Revision Date:	**27 July 2022**

Table of Contents

A. General information about the course:

1. Course Identification

1. Credit hours:					
3 CHrs. (Three-Credit Hours)					
2. Course type					
A.	☐University	☐College	☒ Department	☐Track	☐Others
B.	☒ Required		☐ Elective		
3. Level/year at which this course is offered: (Level 7/4th Year)					
4. Course general Description:					
This course provides the ground-up coverage on the key concepts of information security and its related subdomains. It teaches the main security techniques related to applied cryptography, including the basic operations of symmetric/asymmetric encryptions and the cryptographic hash functions. The course describes the requirements and mechanisms for digital signature and user authentication, and it also outlines the security access controls and their categories (MAC, DAC, RBAC, ABAC). The security threats against database systems along with the security measures for DB inference issues, SQL injection, and preserving database confidentiality are discussed broadly with real-life scenarios. Also, the course highlights the difference between various malicious software types, including viruses, trojan horses, worms, DDoS botnet, spyware, and rootkits. While this course teaches the main principles for intrusion detection and prevention systems and the role of firewalls as part of network security appliances, it also guides the students to fulfill the best practices to secure computer applications and operating systems.					
5. Pre-requirements for this course (if any)**:**					
Computer Networks (CIT 1202) and Database Systems (CIT 1305)					
6. Co-requisites for this course (if any)**:**					
None					
7. Course Main Objective(s):					
Upon the completion of this course the students will be able to: ● Identify the basic concepts in information security. ● Explain the main concepts and functions related to applied cryptography. ● Outline the requirements and mechanisms for digital signature and user authentication. ● Discuss the principal concepts of access controls and their categories. ● Recognize the security threats against database systems and the security measures for DB. ● Distinguish the types of malicious software. ● Recognize the roles of intrusion detection systems and the firewalls for network security. ● Fulfill the best practices to secure computer applications and operating systems.					

2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	**45**	**100%**

No	Mode of Instruction	Contact Hours	Percentage
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**	
5.	**Others (specify)**	
Total		**45**

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

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Define computer and information security terminologies	K1	Lectures. Review papers Supplemental notes In class discussions Supplemental martials to the textbook Office hours	Exams Quizzes Homework's Classwork
1.2	Describe cryptography concepts and techniques	K1		
1.3	Outline program security, operating systems security, and database security	K2		
1.4	Recognize network security techniques and web security	K2 and K3		
1.5	Summarize management of security and Security policies	K4		
2.0	**Skills**			
2.1	Explain the objectives of computer and information security	S1	Lectures. Review papers Supplemental notes	Exams. Assignments. Quizzes.
2.2	Summarize the basic categories of threats to computers and networks	S1		

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
2.3	Analyze the requirements and techniques for security management	S2	In class discussions Supplemental martials to the textbook Office hours	
2.4	Explain the requirements for database and web and operating systems security	S1		
2.5	Evaluate the level of security for a policy or object	S2 and S5	Lectures. Research activities Office hours	Assignments Projects
2.6	Use and practice the security aspects in real life	S4		
2.7	Analyze the data integrity tools used in the networking transmission	S2		
2.8	Evaluate the general security level of an organization	S5	Lectures Assignments Projects	Assignments Projects
2.9	Use the appropriate cryptographic tool for the correct computer application	S4		
2.10	Analyze any kind of threats against information systems	S5		
2.11	Construct cryptographic applications by using presented cryptographic tools	S4	Assignments Projects	Assignments Projects
2.12	Illustrate how the secret message and the overt message are calculated	S3		
2.13	Experiment with the security level of an application or computer tool	S3		
2.14	Employ authentication tools in the organization's main software	S3 and S4		
3.0	**Values, autonomy, and responsibility**			
3.1	None			

C. Course Content

No	List of Topics	Contact Hours
1.	Information Security Overview • Computer Security Concepts • Threats, Attacks, and Assets • Security Functional Requirements • Fundamental Security Design Principles	3

	• Attack Surfaces and Attack Trees • Computer Security Strategy	
2.	Cryptography (Part 1) • Confidentiality with Symmetric Encryption • Message Authentication and Hash Functions	3
3.	Cryptography (Part 2) • Public-Key Encryption • Digital Signature	3
4.	User Authentication • Electronic User Authentication Principles • Password-Based Authentication • Token-Based Authentication • Biometric Authentication • Remote User Authentication • Security Issues for User Authentication	3
5.	Access Control • Access Control Principles • Subjects, Objects, and Access Rights • Discretionary Access Control • Example: Unix File Access Control • Role-Based Access Control • Case Study: RBAC System	3
6.	Database security (Part 1) • The Need for Database Security • Relational Databases and DBMS • SQL Injection	3
7.	Database security (Part 2) • Database Access Control • DB Inference Issue • Database Encryption	3
8.	Malicious Software • Types of Malicious Software (Malware) • Advanced Persistent Threat • Propagation—Viruses • Propagation—Worms • Spam E-Mail and Trojans • Attack Agent: Zombie and Bots • Theft: Keyloggers, Phishing, and Spyware • Stealthy: Backdoors and Rootkits • Countermeasures	3
9.	Denial-of-Service Attacks • Overview: Denial-of-Service (DoS)Attacks • Flooding Attacks • Distributed Denial-of-Service Attacks • Application-Based Bandwidth Attacks	3

	• Reflector and Amplifier Attacks • Defenses Against Denial-of-Service Attacks • Responding to a Denial-of-Service Attack	
10.	Intrusion Detection (Part 1) • Intruders • Intrusion Detection • Analysis Approaches • Host-Based Intrusion Detection • Network-Based Intrusion Detection	3
11.	Intrusion Detection (Part 2) • Distributed or Hybrid Intrusion Detection • Intrusion Detection Exchange Format • Honeypots • Example System: Snort	3
12.	Firewalls and Intrusion Prevention Systems (Part 1) • The Need for Firewalls • Firewall Characteristics and Access Policy • Types of Firewalls	3
13.	Firewalls and Intrusion Prevention Systems (Part 2) • Firewall Basing • Firewall Location and Configurations • Intrusion Prevention Systems	3
14.	Operating System Security (Part 1) • Introduction to Operating System Security • System Security Planning • Operating Systems Hardening • Application Security	3
15.	Operating System Security (Part 2) • Security Maintenance • Linux/Unix Security • Windows Security	3
Total		**45**

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments and Quizzes	3, 5, 9	10%
2.	Midterm Test-1	6 - 7	20 %
3.	Midterm Test-2	12 - 13	20 %
4.	Group Project	7-13	10 %
6.	Final Exam	16-17	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	• William Stallings and Lawrie Brown, Computer Security: Principles and Practice, 3rd ed., Pearson Education, 2015, ISBN: 978-0-13-479410-5
Supportive References	• Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing" 4/E, Prentice Hall 2007, ISBN-13: 9780132390774 • Michael Goodrich, Roberto Tamassia, Introduction to Computer Security , Addison-Wesley 2011, ISBN-13: 9780321512949 • William Stallings, Cryptography and Network Security, sixth edition • William Stallings, Computer Security, Second edition • RFC – Request For Comments • ISO27001 standard
Electronic Materials	• www.ietf.org • https://ieeexplore.ieee.org • https://dl.acm.org/
Other Learning Materials	• Computer operating system: Linux (e.g., Kali Linux) • Software tools: Snort, Nessus, Nmap

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms and LABs
Technology equipment (projector, smart board, software)	Data Show
Other equipment (depending on the nature of the specialty)	Each student should has a laptop with the required Software

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of Teaching	Faculty, Program Leaders, and Advisory Board	Both Direct and Indirect
	Students	Indirect
Effectiveness of Students Assessment	Faculty, Program Leaders, Advisory Board, and Independent Opinion	Both Direct and Indirect
Quality of Learning Resources	Faculty, Students, and Advisory Board	Indirect
The Extent to which CLOs have been Achieved	Faculty, Program Leaders, Advisory Board, and Independent Opinion	Direct (as in section B) and Indirect/Surveys
	Students	Indirect

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

Assessment Methods (Direct, Indirect)

G. Specification Approval

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	