Course Specifications

Course Title:	**Systems Security**
Course Code:	**IT 443**
Program:	
Department:	
College:	
Institution:	

Table of Contents

A. Course Identification

1. Credit hours:	3(2+2)
2. Course type	
a.	University ☐ College ☐ Department ■ Others ☐
b.	Required ■ Elective ☐
3. Level/year at which this course is offered:	
4. Pre-requisites for this course (if any)**:**	Cyber Security Essentials (IT 326)
5. Co-requisites for this course (if any)**:**	Nil

6. Mode of Instruction (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	**Traditional classroom**		80%
2	**Blended**		
3	**E-learning**		20%
4	**Correspondence**		
5	**Other**		

7. Actual Learning Hours (based on academic semester)

No	Activity	Learning Hours
Contact Hours		
1	**Lecture**	
2	**Laboratory/Studio**	
3	**Tutorial**	
4	**Others** (specify)	
	Total	
Other Learning Hours*		
1	**Study**	
2	**Assignments**	
3	**Library**	
4	**Projects/Research Essays/Theses**	
5	**Others** (specify)	
	Total	

* The length of time that a learner takes to complete learning activities that lead to achievement of course learning outcomes, such as study time, homework assignments, projects, preparing presentations, library times

B. Course Objectives and Learning Outcomes

1. Course Description

This course introduces the concepts and principles of system and software components security. It focuses to acquire knowledge of component design security, principles of secure component design, side-channel attack mitigation, anti-tamper technologies, software component interfaces, and connection attacks.

2. Course Main Objectives

1-To understand and apply the concepts and principles of system and software components security.
2-To understand and acquire knowledge of Component design security.
3-To understand describe, analyze and apply the principles of secure component design.
4-To understand and apply the various Side-channel attack mitigation.
5-To understand and apply the basics of anti-tamper technologies.
6-To understand and apply in depth knowledge of software component interfaces, and connection attacks.

3. Course Learning Outcomes

CLOs		Aligned PLOs
1	**Knowledge:**	
1.1	Be able to define and describe the advanced principles of system and software components security.	
1.2	Be able to assess attack strategies through the use of analysis techniques and recommend defenses to those attacks.	
1.3	Be able to define the concept of component design and component design security.	
2	**Skills :**	
2.1	Analyze common intrusion patterns to identify potential attack vectors in order to strategically enhance defenses.	
2.2	Propose appropriate data sources and create methods of analysis in order to aid in tracking and detection of attacks.	
3	**Competence:**	
3.1	Determine appropriate controls to detect suspicious behavior within systems and networks in order to provide recommendations to leadership.	

C. Course Content

No	List of Topics	Contact Hours
1	Introduction to vulnerabilities of system components, Component lifecycle, Secure component design principles.	4
2	Security of component design artifacts (e.g., schematics, netlists, and masks) such as hardware Trojans, intellectual property piracy, reverse engineering, tampering, ML and DCL.	8
3	Component design security: Threats to the security of component design artifacts (e.g., schematics, netlists, and masks) such as hardware Trojans, intellectual property piracy, reverse engineering, tampering, side-channel analysis and counterfeiting. It also introduces techniques for protecting components from unauthorized access and use.	8
4	Principles of secure component design: Basics of security policy, treating security as an integral part of system design, trusted computing platforms, chain of trust, reducing risk, layered security, simplicity of design, minimizing system elements to be trusted, and avoiding unnecessary security mechanisms.	8
5	Side-channel attack mitigation: Techniques for defending against side-channel attacks primarily targeted at cryptographic algorithms. Defensive techniques include leakage reduction, noise injection,	8

	frequent key updates, physical random functions, and secure scan chains.	
6	Anti-tamper technologies: Techniques for making components resistant to physical and electronic attacks including physical protection techniques, tamper evident systems and tamper responding systems.	4
7	Software component interfaces: Explain why every physical interface has a corresponding software component to provide a corresponding software interface. Describe how a specified standard interface could expose vulnerabilities in a software component that implements the interface. Discuss how the Internet 5-layer model can be viewed as software components and interfaces that represent levels of services encapsulated by lower-level services. Discuss how TCP/IP as a service is represented by different interfaces in different software systems.	12
8	Connection attacks: Explain how connection attacks can be understood in terms of attacks on software component interfaces. Describe how a specified standard interface could expose vulnerabilities in a software component that implements the interface. Describe how an implementation could protect itself from a specified vulnerability in a specified standard interface.	8
Total		

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	**Knowledge**		
1.1	Demonstrate an understanding of the core concepts of systems security and encryption systems.	-Lecture -Group Discussions -Presentations	-Assignments -Case study -Project
1.2	Identify and explain the vulnerabilities of information system as well mitigations to information system attacks.		
2.0	**Skills**		
2.1	Gain hands-on experience with attack and defense techniques.	-Lecture -Group Discussion -Presentations	-Assignments -Case study -Project
2.2	Distinguish between viruses and malware, and discuss their impact on personal privacy and computers.		
2.3	Have the ability to specify security policies including: protected resources, defined procedures and available technologies and the role of people involved in the procedure		
2.4	The ability to determine the computer security strategy, the location of these systems administrator.		
3.0	**Competence**		
3.1	Practice cyber safety techniques to protect your computer system when		

Code	Course Learning Outcomes	Teaching Strategies	Assessment Methods
	using Internet searches, e-mail, and social networks websites.		

2. Assessment Tasks for Students

#	Assessment task*	Week Due	Percentage of Total Assessment Score
1	First written mid-term exam	6	20%
2	Second written mid-term exam	12	20%
3	Presentation, class activities, lab activity, and group discussion	Every week	10%
4	Homework assignments	After every chapter	10%
5	Final written exam	15	40%
6	**Total**		100%

***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 :

A total of 6 office hours per week in the lecturer schedule in order to facilitate the student.
Contacting students using the following E-mail address:

fatma_harby@yahoo.com

F. Learning Resources and Facilities

1.Learning Resources

Required Textbooks	William Stallings, Lawrie Brown, "Computer Security Principles and Practice", 2015.
Essential References Materials	Chuck Easttom,Computer Security Fundamentals",2012.
Electronic Materials	https://www.journals.elsevier.com/computers-and-security
Other Learning Materials	

2. Facilities Required

Item	Resources
Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.)	- Furnished with a large central table or multiple small tables that can be grouped into one central table - Designed for up to 25 students - Size the room allowing 1sq meter per seat

Item	Resources
Technology Resources (AV, data show, Smart Board, software, etc.)	- Smart Board, projector, internet, and whiteboard.
Other Resources (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list)	None

G. Course Quality Evaluation

Evaluation Areas/Issues	Evaluators	Evaluation Methods
Strategies for Obtaining Student Feedback on Effectiveness of Teaching	- Student questionnaires to be assessed by independent body. -Assessment of course teaching strategies by independent body.	
Evaluation of Teaching by the Program/Department Instructor:	-Student questionnaires to be assessed by department.	
Verifying Standards of Student Achievement.	-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)	
Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.	-Reviewing student's feedback. Update text books. -Consulting other top universities course specifications and contents.	

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

Council / Committee	
Reference No.	
Date	