CS3273: DATA PROTECTION AND SYSTEM SECURITY

Effective Term

Semester A 2023/24

Part I Course Overview

Course Title

Data Protection and System Security

Subject Code

CS - Computer Science

Course Number

3273

Academic Unit

Computer Science (CS)

College/School

College of Engineering (EG)

Course Duration

One Semester

Credit Units

3

Level

B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction

English

Medium of Assessment

English

Prerequisites

CS2311 Computer Programming or
CS2315 Computer Programming or
CS2334 Data Structures for Data Science or equivalent

Precursors

Nil

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

This course is aimed at developing a solid understanding in data privacy, protection and system security for students with no or little knowledge of computer system and network architectures. Student will acquire adequate understanding on different components in operating systems and network, be able to identify threats at different levels, acquire skill to specify and evaluate appropriate security measures for attacks. These skills will then be applied to address issues of data privacy, security and integrity. Available and emerging tools for attack, intrusion detection, access control and data protection will also be introduced.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Acquire basic knowledge of operating systems, structure and non-structure databases and networks in the context of security and protection.		x	x	
2	Identify, classify and analyze common threats and vulnerabilities of network, computer and big data		x	x	
3	Suggest and evaluate major countermeasures for software and web application, network and big data attacks.			x	
4	Use and analyse existing and emerging tools for system and network security, and data protection.			x	

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Teaching and Learning Activities (TLAs)

	TLAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	The different types of attacks to software, web systems, network and databases will be introduced. Principles, techniques and technologies used for defending against these attacks will be discussed. Selected available and emerging tools for attack, access control, network and data protection will also be introduced.	1, 2, 3, 4	3 hours/week
2	Tutorial	Tutorials will be conducted in laboratory in the forms of discussion, demonstration, and hands-on sessions. Students will work with selected security and attacking tools. This provides students with hands-on experience in using, configuring the tools and analysing how the security and attacking tools work. With these exercises, student will know how the adversary makes use of the tool to attack software, web systems and databases, and how to engineer secure network, software and databases. Students will then be able to identify and analyse potential threats to organizations and formulate plans for organizations to defend themselves. This helps support Course ILO #1, #2, #3 and #4.	1, 2, 3, 4	8 hours/semester

3	Case Studies	Students will be provided with different attack scenarios and are required to identify the security threats, evaluate and critically analyse the security counter measures. This activity helps support Course ILO #1, #2, #3 and #4.	1, 2, 3, 4	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Coursework: Three assignments and one mid-term quiz	1, 2, 3, 4	50	

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Coursework

Criterion

Questions and hands-on exercises to assess the students' understanding of the different components in the cyberspace and system attacks, related defences, and relevant tools for secure computation. Students are required to generate reports to summarize their findings.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Assessment Task

Examination

Criterion

The exam will include questions to assess the student’ s ability to explain how various attacks work, the understanding of the principles, techniques and technologies used for defending against various attacks.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

Overview of operating system, network, Internet, the Web, cloud, structured, non-structured and big data; Operating system security, access control; Identity and credential management; Program control hijacking and defence, malicious codes and virus; Network security; Big Data security, privacy and accountability; Evaluating system security, secure computing platforms; Secure computation techniques.

Syllabus

- Overview of systems, network and big data management:
  - Operating systems
  - Network, Internet, the Web and Cloud
  - Big Data management
- Software and network security:
  - Phases in launching an attack
  - Software and network attacks and countermeasures
  - Internet and Web system attacks and countermeasures
- Big Data security:
  - Basic data security, file access control and secure network protocols
  - Reliable and secure data access for Big Data service
  - Cryptography for data security
- Big Data privacy and accountability:
  - Privacy and accountability concerns in Big Data
  - Privacy preserving in Big Data and data analytics
  - Big Data quality and governance
- Tools for:
  - System and network attack
  - Intrusion detection and monitoring

- Secure networking and computation
- Data encryption, integrity and availability

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	Rhodes-Ousley (2013). Information security: the complete reference, McGraw-Hill. 2nd edition.
2	Hu Fei ed (2016). Big data : storage, sharing, and security, CRC Press