CS2117: FOUNDATION OF CYBERSECURITY

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Foundation of Cybersecurity

Subject Code
CS - Computer Science
Course Number
2117

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

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

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course aims to provide a fundamental understanding of cybersecurity principles. Students will gain a broad understanding in a wide array of cybersecurity aspects, including but not limited to risk, ethics, cryptography, web and network security.
Students are given the opportunity to identify and discuss security requirements of current systems, identify potential security problems, evaluate the performance of existing approaches and design appropriate security policy and controls for everyday systems

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify and explain the requirements of secure systems.		x	x	
2	Assess security threats against systems from various attacks and identify potential security problems.		x	x	
3	Evaluate and critique the security and performance of existing security mechanisms and systems.			x	
4	Design of secure systems using learnt security mechanisms and principles.		x	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.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Students will gain understanding on key topics of cybersecurity. Additional examples and case studies will be discussed.	1, 2, 3, 4	3 hours/week
2	Tutorials	Students will collaborate to solve problem sets and complete additional exercises related to lecture content.	1, 2, 3, 4	8 hours/semester
3	Assignments	Students will apply their knowledge to solve selected theoretical and practical problems related to course topics.	1, 2, 3, 4	

4	Quiz	Quiz to evaluate the students' understanding of course topics.	1, 2, 3, 4	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignments	1, 2, 3, 4	20	3 Problem Sets	Yes
2	Mid-term Test	1, 2, 3, 4	10	-	No

Continuous Assessment (%)
30

Examination (%)
70

Examination Duration (Hours)
2

Minimum Examination Passing Requirement (%)
30

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
Assignments

Criterion
Exhibit understanding of information security principles in evaluating and designing secure systems

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
Mid-term Test

Criterion
Ability to explain and apply information security principles

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
Ability to explain information security principles and also demonstrate the ability to evaluate and design aspects of secure systems

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
A selection of topics from the following: system security, network security, computer security, web security, access control, firewall, intrusion detection systems, cryptography, symmetric encryption, asymmetric encryption digital signature, message authentication, hash functions, PKI, ethics and disclosure.

Syllabus

A selection of topics from the following:

- System security: Principles of secure systems, including security services, risk, ethics and legal issues.
- Network, web and computer security: Basic notions and techniques of access control, firewalls, DDoS, phishing attacks, web security exploits, and related subjects.

- Cryptographic techniques:Classic cryptography, symmetric and asymmetric encryption, digital signature, message authentication, cryptographic hash functions
- Security protocols and systems: Authentication protocols, PKI, certificate authority, TLS, cryptocurrency

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	Stallings W. (2020). Cryptography and Network Security: Principles and Practice. Prentice Hall. 8th edition.
2	Anderson R. (2020). Security Engineering. Wiley, 3rd edition.