

# CS4293: TOPICS IN CYBERSECURITY

---

## Effective Term

Semester A 2025/26

## Part I Course Overview

### Course Title

Topics in Cybersecurity

### Subject Code

CS - Computer Science

### Course Number

4293

### 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

(CS2310 Computer Programming or  
CS2311 Computer Programming or  
CS2312 Problem Solving and Programming or equivalent)  
and (CS3103 Operating Systems or equivalent)  
and (CS3201 Computer Networks or equivalent)

### Precursors

Nil

### Equivalent Courses

Nil

### Exclusive Courses

Nil

## Part II Course Details

### Abstract

This course is aimed at developing students a solid understanding in a range of topics in the area of cybersecurity. Student will acquire adequate understanding on threats of web applications and network, acquire skill to specify and evaluate appropriate security measures for computer systems and software applications, and get familiar with emerging privacy-enhancing technologies such as Bitcoin-like cryptocurrencies, blockchain and decentralised applications, and secure computation.

### Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify and analyze common threats and vulnerabilities of software and web applications.		x	x	
2	Classify and analyze common threats and vulnerabilities of network and systems.		x	x	
3	Explain and evaluate major countermeasures to software and web application, network and system attacks			x	
4	Describe and analyse emerging privacy-enhancing technologies including cryptocurrencies, blockchain and decentralised applications, and secure computation.			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	Lecture	Students will learn different types of attacks on software, web applications, network, and systems will be introduced. Principles, techniques, and technologies used for defending against these attacks will be discussed. Selected topics of emerging privacy-enhancing technologies will also be presented, including cryptocurrencies, blockchain, decentralised applications, and secure computation.	1, 2, 3, 4 3 hours/week
2	Tutorial	Students will take the tutorials in the laboratory through discussion, demonstration, and hands-on sessions. Students will work with selected security and attacking tools. This provides students with hands-on experience in using and configuring the tools and analysing how the security and attacking tools work. With these exercises, students will know how the adversary uses the tool to attack software and web applications and how to engineer secure software that interacts with cryptocurrencies and their extended applications. Students will be able to identify and analyse potential threats to computer systems in organizations and formulate solutions as to how organizations may 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 and evaluate and critically analyse the security systems. This activity helps support Course ILO #1, #2, #3, and #4.	1, 2, 3, 4	After class
---	--------------	--	------------	-------------

**Assessment Tasks / Activities (ATs)**

ATs	CILO No.	Weighting (%)	Remarks ("- " for nil entry)	Allow Use of GenAI?	
1	Coursework: Three assignments and one mid-term quiz	1, 2, 3, 4	50	-	No

**Continuous Assessment (%)**

50

**Examination (%)**

50

**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**

Coursework

**Criterion**

Questions and hands-on exercises to assess the students' understanding of the different types of software, web application, network and system attacks, related defences, and the concept and design principle of cryptocurrencies, blockchain and decentralised applications, and 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, and the ability to describe and analyse emerging privacy-enhancing technologies.

### **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**

The syllabus will evolve over time as current topics change. The following are example keyword syllabus: Cryptographic tools and their usage in practical settings; OS security, file system protection, access control; Identity and credential management; Memory safety, program control hijacking and defence, malicious codes, virus; Network security; Probing tools; Evaluating system security, secure computing platforms; Bitcoin; Cryptocurrencies; Blockchain and decentralised applications; Secure computation techniques.

Syllabus

- Selected topics in computer security:
  - Cryptographic tools and their usage in practical settings
  - Identity and credential management.
  - File system protection, access control
- Software security
  - Software attacks and countermeasures
  - web application attacks and countermeasures
- Network Security
  - Network attacks and countermeasures
  - Phases in launching an attack and countermeasures
- Other emerging topics:
  - Cryptocurrencies
  - Blockchain and decentralised applications
  - Secure computation

### **Reading List**

### Compulsory Readings

Title	
1	Nil

### Additional Readings

Title	
1	Stallings and Brown (2012). Computer Security- Principles and Practice. 2e, Pearson. Int' l edition.
2	Goodrich and Tamassia (2011/2014). Introduction to Computer Security. 1e, Pearson. Int' l edition.