CS5293: TOPICS IN INFORMATION SECURITY AND PRIVACY

Effective Term
Semester A 2026/27

Part I Course Overview

Course Title
Topics in Information Security and Privacy

Subject Code
CS - Computer Science
Course Number
5293

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
CS5285 Information Security for eCommerce or equivalent

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course aims to provide students with a solid understanding of a range of topics in the field of information security, with emphasis on identification of security threats to actual systems and the appropriate countermeasures. On completion of the course students should be able to acquire adequate understanding on threats of web applications and network and acquire skill to specify and evaluate appropriate security measures for computer systems and software applications.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify and analyse common threats and vulnerabilities of software and web applications.	25	x	x	x
2	Classify and analyse common threats and vulnerabilities of network and systems.	20	x	x	
3	Suggest and evaluate major countermeasures to software web application, network and system attacks.	25	x	x	x
4	Identify and enquire security issues in emerging computing technology and applications.	30	x	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 learn different types of attacks to software, web applications, network, and system. Students will also learn the defence principles, techniques, and technologies used for these attacks. Additional selected timely security issues in the emerging computing technology will also be covered.	1, 2, 3, 4	2 hours/ week

2	Tutorials	Students will discuss, watch demonstrations, and work with selected security and attacking tools in the lab which provide students with hands-on experience in using and 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 and web 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.	1, 2, 3, 4	1 hour/ week
3	Project	Students will be asked to conduct a substantial case study or in-depth survey on selected security topics, such as thoroughly analysing the security properties of crypto techniques in some system/network protocols, advanced access control, passwords and related usages, memory safety issues and defences, web tracking, command injection attacks and defences, cloud security, etc.	1, 2, 3, 4	2 hours/ week for 4 weeks

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignment 1	1, 2	13	-	No
2	Assignment 2	2, 3	13	-	No
3	Assignment 3	3, 4	13	-	No
4	Project	1, 2, 3, 4	11	-	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

Problem set, including assignments and examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Ability to answer fundamental network or information security attacks and defences.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Below Marginal

Assessment Task

Hands-on exercises (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Capacity to explore open-source security toolkit and perform hands-on exercises, as well as explore the attack and defence technologies on software, system, and web.

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Below Marginal

Assessment Task
Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to conduct a substantial case study or in-depth survey on selected security topics.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Below Marginal

Assessment Task
Problem set, including assignments and examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to answer fundamental network or information security attacks and defences.

Excellent
(A+, A, A-) High

Good
(B+, B) Significant

Marginal
(B-, C+, C) Basic

Failure
(F) Below Marginal

Assessment Task
Hands-on exercises (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Capacity to explore open-source security toolkit and perform hands-on exercises, as well as explore the attack and defence technologies on software, system, and web.

Excellent
(A+, A, A-) High

Good
(B+, B) Significant

Marginal
(B-, C+, C) Basic

Failure
(F) Below Marginal

Assessment Task
Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to conduct a substantial case study or in-depth survey on selected security topics.

Excellent
(A+, A, A-) High

Good
(B+, B) Significant

Marginal
(B-, C+, C) Basic

Failure
(F) Below Marginal

Part III Other Information

Keyword Syllabus
The syllabus will evolve over time as current topics change. Current topics will be selected from following. 1) Software security: Cryptographic toolkit with correct parameter settings in practice, memory safety, software attacks and countermeasures. 2) Web security: web application attacks and countermeasures, isolation and same origin policy, command injection identification, and defence. 3) Network Security: network attacks and countermeasures, intrusion detection systems, phases in launching an attack and countermeasures. 4) Other topics in computer security and privacy: cloud security, security policy, information privacy, computer crime, new access control paradigms, and data security.

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	M. Goodrich and R. Tamassia. Introduction to Computer Security. Pearson. (2014)
2	W. Stallings and L. Brown. Computer Security: Principles and Practice. (2015)
3	Shah S. Web 2.0 security: Defending Ajax, RIA, and SOA. Thomson (2008)
4	Spitzner L. Honeypot: Tracking hackers. Addison-Wesley (2003)

5	Bace R. G. Intrusion Detection. Macmillan Technical (2000)
6	Whittaker and Thompson. How to break software security. Addison Wesley (2004)
7	Andrews and Whittaker. How to break web software. Addison Wesley (2006)
8	Skoudis and Liston, Counter Hack Reloaded (2e). Prentice Hall (2006)