CS5285: INFORMATION SECURITY FOR ECOMMERCE

Effective Term

Semester A 2025/26

Part I Course Overview

Course Title

Information Security for eCommerce

Subject Code

CS - Computer Science

Course Number

5285

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

Nil

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

The course aims to provide an understanding of information security, giving an overview of the requirements and means for the protection of data and systems and, which is an essential feature in the design of eCommerce systems. The course also examines a range of information security considerations and design issues that are incorporated into the design, development and management of the eCommerce systems.

Course Intended Learning Outcomes (CILOs)

	CILOs	**Weighting (if app.)**	**DEC-A1**	**DEC-A2**	**DEC-A3**
1	Identify and explain the organizational requirements of eCommerce systems on data protection.		x	x	x
2	Demonstrate knowledge of the factors which have impacts upon the security of eCommerce systems.			x	
3	Apply formulated strategies to assess the security of eCommerce systems.		x	x	
4	Describe relevant regulations governing electronic transactions, data privacy protection, and web access.			x	
5	Design and analyze security mechanisms to protect eCommerce systems and transactions.		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 engage with key concepts of information security. Fundamental principles will be illustrated with real world examples.	1, 2, 3, 4, 5	2 hours/week
2	Tutorials	Students will work on solving information security problems to reenforce understanding of lecture material.	1, 2, 3, 4, 5	1 hour/week

3	Problem Sets	Students will individually apply course concepts to evaluate and create secure systems. Some problems could provide the opportunity to discover how current secure systems operate.	1, 2, 3, 4, 5	4 hr/wk for 4 weeks

Additional Information for LTAs

Lectures- CILO No.1-6 (indirectly)

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Problem Set 1	1, 2, 3, 4, 5	10	-	Yes
2	Mid-term Test	1, 2, 3, 4, 5	20	-	No
3	Problem Set 2	1, 2, 3, 4, 5	10	-	Yes

Continuous Assessment (%)

40

Examination (%)

60

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

Mid-term Test (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

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

Problem Sets (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Identify and apply 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

Problem Sets (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Demonstrate ability to identify information security principles in real-world applications.

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

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

Criterion

Ability to describe, analyse and apply concepts related to information security principles and 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 (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to explain and apply information security principles.

Excellent

(A+, A, A-) High

Good

(B+, B) Significant

Marginal

(B-, C+, C) Moderate

Failure

(F) Not even reaching marginal levels

Assessment Task

Problem Sets (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Identify and apply information security principles in evaluating and designing secure systems.

Excellent

(A+, A, A-) High

Good

(B+, B) Significant

Marginal

(B-, C+, C) Moderate

Failure

(F) Not even reaching marginal levels

Assessment Task

Problem Sets (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Demonstrate ability to identify information security principles in real-world applications.

Excellent

(A+, A, A-) High

Good

(B+, B) Significant

Marginal

(B-, C+, C) Moderate

Failure

(F) Not even reaching marginal levels

Assessment Task

Exam (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to describe, analyse and apply concepts related to information security principles and systems

Excellent

(A+, A, A-) High

Good

(B+, B) Significant

Marginal

(B-, C+, C) Moderate

Failure

(F) Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

A selection of topics from the following: overview of information security; risks and attacks, security policies and mechanisms; access control, cryptographic techniques, public key infrastructures, authentication and digital certificates; detection and audit; security enforcement in electronic commerce; information security management and standards; privacy protection techniques and regulations, ethical web posting, hosting and surfing.
Syllabus:
A selection of topics from the following:
1. Overview of information security for eCommerce systems
· Attacks against eCommerce systems, that include malicious software, network attacks (e.g. DDoS), phishing attack, password guessing attack, etc.
· eCommerce protection systems: firewall, intrusion detection system, access control mechanisms.
· Security policies for eCommerce systems, information security management and standards.
· Critique and assessment of security measures.
2. Cryptographic techniques

- Symmetric-key cryptography, public key cryptography.
- Public Key Infrastructure, authentication and digital certificates, electronic transaction ordinance.

3. eCommerce protocols and schemes

- Secure email protocols and schemes.
- Secure web browsing, online banking, online shopping and similar eCommerce systems.
- Fundamental cryptographic protocols for eCommerce systems: SSL, IPSec, IKE, SET.
- Security protocol design
- Techniques and ethics in web and privacy data protection.

4. Topics on secure eCommerce systems

- Electronic cash, electronic auction, payment systems.
- Intellectual property protection techniques.

Reading List

Compulsory Readings

	Title
1	Stallings W. Cryptography and Network Security: Principles and Practice. 6th Ed. Prentice Hall (2013)

Additional Readings

	Title
1	Stinson D. R. Cryptography - Theory and Practice. 3rd Ed. CRC Press (2005)
2	Anderson R. Security Engineering. 2nd Ed. Wiley (2008)
3	Stamp M. Information Security: Principles and Practice. Wiley (2011)