City University of Hong Kong
Course Syllabus

offered by Department of Computer Science
with effect from Semester A 2017/18

Part I Course Overview

Course Title:	Information Security for eCommerce
Course Code:	CS5285
Course Duration:	One semester
Credit Units:	3 credits
Level:	P5
Medium of Instruction:	English
Medium of Assessment:	English
Prerequisites: *(Course Code and Title)*	Nil
Precursors: *(Course Code and Title)*	Nil
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. 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.

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs	Weighting (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Identify the organizational requirements of eCommerce systems on data protection.		√	√	√
2.	Demonstrate knowledge of the factors which have impacts upon the security of eCommerce systems.			√	
3.	Make critique and assessment on the security of eCommerce systems.		√	√	
4.	Describe relevant regulations governing electronic transactions, data privacy protection, and web access.			√	
5.	Create design and analyze security mechanisms to protect eCommerce systems and transactions.		√	√	√
		100%			

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 self-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.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

Teaching pattern:
Suggested lecture/tutorial/laboratory mix: 2 hrs. lecture; 1 hr. tutorial.

TLA	Brief Description	CILO No.					Hours/week (if applicable)
		1	2	3	4	5	
Lectures	Explain and discuss the key concepts of information security.	√*	√*	√*	√*	√*	2 hr/wk
Tutorials	Class exercises for enforcing basic concepts and applying these to information security problems.	√	√	√	√	√	1 hr/wk
Problem Sets	Requires students to individually apply course concepts to evaluate and create secure systems. Some problems could provide the opportunity to discover how current secure systems operate.	√	√	√	√	√	4 hr/wk for 4 weeks

***** indirectly

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

Assessment Tasks/Activities	CILO No.					Weighting	Remarks
	1	2	3	4	5		
Continuous Assessment: <u>40</u>%							
Problem Set 1	√	√	√	√	√	10%	
Mid-term Test	√	√	√	√	√	20%	
Problem Set 2	√	√	√	√	√	10%	
Examination^: <u>60</u>% (duration: 2 hours)							
						100%	

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

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
1. Mid-term Test	Ability to explain and apply information security principles.	High	Significant	Moderate	Basic	Not even reaching marginal levels
2. Problem Sets	Exhibit understanding of information security principles in evaluating and designing secure systems.	High	Significant	Moderate	Basic	Not even reaching marginal levels
	Demonstrate ability to engage with information security principles in real-world applications.	High	Significant	Moderate	Basic	Not even reaching marginal levels

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

(An indication of the key topics of the course.)

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.

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

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

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

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)