

City University of Hong Kong

**Information on a Course
offered by Department of Computer Science
with effect from Semester A in 2012 / 2013**

Part I

Course Title: Information Security for eCommerce

Course Code: CS5285

Course Duration: One Semester

Credit Units: 3

Level: P5

Medium of Instruction: English

Prerequisites: Nil

Precursors: CS5222 Computer Networks and Internets or equivalent

Equivalent Courses: Nil

Exclusive Courses:

For MSc Computer Science and MSc Electronic Commerce programmes, CS5285 Information Security for eCommerce is exclusive with CS6287 Network and Information Security.

Part II

Course Aims

The course provides an overview of the requirements and means for the protection of data during processing, storage and transmission, which is an essential feature in the design of eCommerce systems. The course also examines the 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)

Upon successful completion of this course, students should be able to:

| No. | CILOs | Weighting (if applicable) |
|-----|-------------------------------------------------------|------------------------------|
| 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. | |

Teaching and Learning Activities (TLAs)

(Indicative of likely activities and tasks designed to facilitate students' achievement of the CILOs. Final details will be provided to students in their first week of attendance in this course)

Teaching pattern:

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

Based on the Course ILOs, the teaching/learning activities of this course include traditional lectures and tutorial sessions. Take-home problem sets and tutorial exercises will be given to help students comprehend materials covered in lectures.

| CILO No. | TLAs | Hours/week (if applicable) |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| CILO 1 | Course ILO #1 will be introduced and explained in lectures. Tutorial and problem set questions will help students attain this ILO. | |
| CILO 2 | Actual cases introduced in tutorials will help students attain this Course ILO. Through studying the cases in tutorials, students are going to learn and demonstrate their knowledge on identifying and exploring various factors that have significant impacts on the security of eCommerce systems. | |
| CILO 3 | Various eCommerce systems will be introduced in lectures and tutorials. Students will learn how to assess the security of the systems. Related problem set questions will also be given for providing students with more concrete practice on the methods of security assessment. | |
| CILO 4 | Various regulations and techniques will be introduced in lectures with case examples discussed and analyzed in tutorials. | |
| CILO 5 | Techniques for achieving this Course ILO will be taught in lectures. In tutorial sessions, students will be | |

| | | |
|--|-----------------------------------------------------------------------------------------------------------------------------------|--|
| | asked to apply the techniques to design security measures and protocols for protecting eCommerce systems and analyse the results. | |
|--|-----------------------------------------------------------------------------------------------------------------------------------|--|

Assessment Tasks/Activities

(Indicative of likely activities and tasks designed to assess how well the students achieve the CILOs. Final details will be provided to students in their first week of attendance in this course)

| CILO No. | Type of Assessment Tasks/Activities | Weighting (if applicable) | Remarks |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------|
| CILO 1 | Coursework, which include take-home problem sets and in-class quizzes, and examination will be given to evaluate this ILO. | | |
| CILO 2 | Coursework and examination will be given to evaluate this ILO. | | |
| CILO 3 | Coursework and examination questions will be made up to evaluate whether students are able to identify the security problems of the systems described in the questions. | | |
| CILO 4 | In-class quiz and coursework assignment questions are used to assess student's attainment of this ILO. | | |
| CILO 5 | Mini-project and coursework on designing and analyzing security mechanisms for eCommerce systems will be used. Exam questions will also include questions on analysing security problems and measures. | | |

Grading of Student Achievement: Refer to Grading of Courses in the Academic Regulations for Taught Postgraduate Degrees.

Examination duration: 2 hours

Percentage of coursework, examination, etc.: 40% CW; 60% Exam

Grading pattern: Standard (A+AA-...F)

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

Part III

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.

Recommended Reading

Text(s)

Stallings W. *Cryptography and Network Security: Principles and Practice, 5th Ed.* Prentice Hall (2010)

Stamp M. *Information Security: Principles and Practice*. Wiley (2011)

Online Resources