**City University of Hong Kong**
**Course Syllabus**

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

---

**Part I Course Overview**

| | |
|---|---|
| **Course Title:** | Internet Security and E-Commerce Protocols |
| **Course Code**: | CS4286 |
| **Course Duration:** | One semester |
| **Credit Units**: | 3 credits |
| **Level**: | B4 |
| **Proposed Area:** *(for GE courses only)* | ☐ Arts and Humanities<br>☐ Study of Societies, Social and Business Organisations<br>☐ Science and Technology |
| **Medium of Instruction:** | English |
| **Medium of Assessment:** | English |
| **Prerequisites**: *(Course Code and Title)* | CS3201 Computer Networks<br>or<br>CS3270 Fundamentals of Computer Networks and the Internet<br>or<br>BCH2808 Forensics and Modern Society<br>(For students intending to take a Minor in Forensic Studies)<br>or<br>equivalent |
| **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

*(A 150-word description about the course)*

This course aims to provide an understanding of information security. Students are expected to gain a broad understanding of information security with the goal of recognising security problems and discovering the security requirements of current computer systems. The course explores existing security mechanisms and offers students the opportunity to evaluate and design techniques for enforcing computer and network security and developing secure e-commerce protocols.

### 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 security requirements of various security systems. | | ✓ | ✓ | |
| 2. | Make critique and assess the security threats of systems against various attacks and identify potential security problems on Internet services and communications. | | ✓ | ✓ | |
| 3. | Create the design of secure e-commerce protocols or systems using cryptographic algorithms and protocols. | | | ✓ | |
| 4. | Evaluate and critique the security and performance of security algorithms and protocols, and e-commerce systems. | | ✓ | ✓ | |
| ** If weighting is assigned to CILOs, they should add up to 100%.* | | 100% | | | |

*[#] Please specify the alignment of CILOs to the Gateway Education Programme Intended Learning outcomes (PILOs) in Section A of Annex.*

*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 | |
| 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 |
| Assignments | 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 | | |
| Continuous Assessment: 30% | | | | | | |
| Assignments | ✓ | ✓ | ✓ | ✓ | 20% | 3 Problem Sets |
| Mid-term Test | ✓ | ✓ | ✓ | ✓ | 10% | |
| Examination^: 70% (duration: 2 hours) | | | | | | |
| ** The weightings should add up to 100%.* | | | | | 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. Assignments | 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 |
| 3. Examination | Ability to explain information security principles and also demonstrate the ability to evaluate and design aspects of secure systems | 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: network security, computer security, malicious software, access control, firewall, intrusion detection systems, classical cryptography, symmetric-key encryption, DES, AES, public key cryptography, digital signature, digital certificate, message authentication, hash functions, RSA, ECC, SHA-1, SHA-256, PKI, authentication and key establishment protocols, SSL, PEM, PGP, IPSec, IKE, e-cash, micropayment, SET, electronic voting, electronic auction, smart card, etc.

Syllabus

A selection of topics from the following:

1. Network security and computer security

   Basic notions and techniques of DDoS, phishing attacks, malicious software such as worms, Trojan horses and viruses, firewall, packet filtering, intrusion detection systems, access control mechanisms and related subjects.

2. Cryptographic techniques

   Classical cryptography, symmetric-key encryption, public key cryptography, digital signature, message authentication, cryptographic hash functions and some concrete algorithms such as DES, AES, RSA, ECC (Elliptic Curve Cryptosystems), SHA-1, SHA-256, HMAC.

3. Security protocols and e-commerce protocols/schemes

   Authentication protocols, password-based authentication, digital certificate, certificate authority, revocation schemes, IPSec, IKE, SET, SSL, e-cash, micropayment, blind signature

4. Advanced cryptographic protocols and e-commerce systems

   Electronic voting, electronic auction, payment servers, secret-sharing schemes, fair exchange of signatures for contract signing

**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. (2013). *Cryptography and Network Security: Principles and Practice.* Prentice Hall. 6th edition. |

**2.2 Additional Readings**

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

| | |
|---|---|
| 1. | Stinson D. R. (2005). *Cryptography - Theory and Practice.* CRC Press, 3rd edition. |
| 2. | Anderson R. (2008). *Security Engineering*. Wiley, 2nd edition. |