City University of Hong Kong
Course Syllabus

offered by Department of Computer Science
with effect from Semester A 2022/23

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
  Study of Societies, Social and Business Organisations
  Science and Technology
Medium of Instruction: English
Medium of Assessment: English
  CS3201 Computer Networks
  CHEM2808 Forensics and Modern Society
  CHEM2809 Science Versus Crime
Prerequisites: (Course Code and Title)
  Nil
  (For students intending to take a Minor in Forensic Studies)
  or 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.)*
   
<table>
<thead>
<tr>
<th>No.</th>
<th>CILOs*</th>
<th>Weighting* (if applicable)</th>
<th>Discovery-enriched curriculum related learning outcomes (please tick where appropriate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify the security requirements of various security systems.</td>
<td>✓ ✓ ✓</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Make critique and assess the security threats of systems against various attacks and identify potential security problems on Internet services and communications.</td>
<td>✓ ✓ ✓</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Create the design of secure e-commerce protocols or systems using cryptographic algorithms and protocols.</td>
<td>✓ ✓ ✓</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Evaluate and critique the security and performance of security algorithms and protocols, and e-commerce systems.</td>
<td>✓ ✓ ✓</td>
<td></td>
</tr>
</tbody>
</table>

* If weighting is assigned to CILOs, they should add up to 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.)

<table>
<thead>
<tr>
<th>TLA</th>
<th>Brief Description</th>
<th>CILO No.</th>
<th>Hours/week (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>The lectures focus on key topics of information security.</td>
<td>✓ ✓ ✓ ✓</td>
<td>3 hours/week</td>
</tr>
<tr>
<td></td>
<td>Additional examples and case studies will be discussed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tutorial</td>
<td>Students work on problems and exercises related to the topics taught in lectures.</td>
<td>✓ ✓ ✓ ✓</td>
<td>8 hours/semester</td>
</tr>
<tr>
<td>Assignment</td>
<td>Assignments provide opportunity to solve selected theoretical and practical problems related to course topics.</td>
<td>✓ ✓ ✓ ✓</td>
<td>After class</td>
</tr>
<tr>
<td>Quiz</td>
<td>Mid-term quiz to evaluate understanding of course topics.</td>
<td>✓ ✓ ✓ ✓</td>
<td></td>
</tr>
</tbody>
</table>

4. Assessment Tasks/Activities (ATs)
(ATs are designed to assess how well the students achieve the CILOs.)

<table>
<thead>
<tr>
<th>Assessment Tasks/Activities</th>
<th>CILO No.</th>
<th>Weighting*</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Assessment: 30%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td>✓ ✓ ✓ ✓</td>
<td>20%</td>
<td>3 Problem Sets</td>
</tr>
<tr>
<td>Mid-term Test</td>
<td>✓ ✓ ✓ ✓</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>Examination : 70% (duration: 2 hours)</td>
<td>✓ ✓ ✓ ✓</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

* The weightings should add up to 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.*

<table>
<thead>
<tr>
<th>Assessment Task</th>
<th>Criterion</th>
<th>Excellent (A+, A, A-)</th>
<th>Good (B+, B, B-)</th>
<th>Fair (C+, C, C-)</th>
<th>Marginal (D)</th>
<th>Failure (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mid-term Test</td>
<td>Ability to explain and apply information security principles</td>
<td>High</td>
<td>Significant</td>
<td>Moderate</td>
<td>Basic</td>
<td>Not even reaching marginal levels</td>
</tr>
<tr>
<td>2. Assignments</td>
<td>Exhibit understanding of information security principles in evaluating and designing secure systems</td>
<td>High</td>
<td>Significant</td>
<td>Moderate</td>
<td>Basic</td>
<td>Not even reaching marginal levels</td>
</tr>
<tr>
<td></td>
<td>Demonstrate ability to engage with information security principles in real-world applications</td>
<td>High</td>
<td>Significant</td>
<td>Moderate</td>
<td>Basic</td>
<td>Not even reaching marginal levels</td>
</tr>
<tr>
<td>3. Examination</td>
<td>Ability to explain information security principles and also demonstrate the ability to evaluate and design aspects of secure systems</td>
<td>High</td>
<td>Significant</td>
<td>Moderate</td>
<td>Basic</td>
<td>Not even reaching marginal levels</td>
</tr>
</tbody>
</table>
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.)*


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