City University of Hong Kong
Course Syllabus

offered by Department of Computer Science
with effect from Semester A in 2015/16

Part I Course Overview

Course Title: Topics on Computer Security

Course Code: CS4293

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

Prerequisites:
(Course Code and Title)
(CS2310 Computer Programming or
CS2311 Computer Programming or
CS2331 Problem Solving and Programming or equivalent)
and (CS3103 Operating Systems or equivalent)
and (CS3201 Computer Networks or equivalent)

Precursors:
(Course Code and Title)
CS4286 Internet Security & E-Commerce Protocols

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 is aimed at developing students a solid understanding in a range of topics in the area of computer and information security. Student will acquire adequate understanding on threats of web applications and network, and acquire skill to specify and evaluate appropriate security measures for computer systems and software applications.

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 and analyze common threats and vulnerabilities of software and web applications.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2.</td>
<td>Classify and analyze common threats and vulnerabilities of network and systems.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3.</td>
<td>Suggest and evaluate major countermeasures to software and web application, network and system attacks.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Identify and enquire current issues in computer security.</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.)*

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

<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 different types of attacks to software, web applications, network and systems will be introduced. Principles, techniques and technologies used for defending against these attacks will be discussed. One of the selected issues in computer security will also be discussed.</td>
<td>✓ ✓ ✓ ✓</td>
<td>2 hrs/wk</td>
</tr>
<tr>
<td>Tutorial</td>
<td>Tutorials will be conducted in laboratory in the forms of discussion, demonstration and hands-on sessions. Students will work with selected security and attacking tools. This provides students with hands-on experience in using, configuring the tools and analyzing how the security and attacking tools work. With these exercises, student will know how the adversary makes use of the tool to attack software and web applications. Students will be able to identify and analyse potential threats to computer systems in organizations and formulate solutions as to how organizations may defend themselves. This helps support Course ILO #1, #2, #3 and #4.</td>
<td>✓ ✓ ✓ ✓</td>
<td>1 hr/wk</td>
</tr>
<tr>
<td>Case Studies</td>
<td>Students will be provided with different attack scenarios and are required to identify the security threats, evaluate and critically analyze the security systems. This activity helps support Course ILO #1, #2, #3 and #4.</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>1 2 3 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coursework: Two assignments and one mid-term quiz</td>
<td>✓ ✓ ✓ ✓</td>
<td>30%</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>Adequate (C+, C, C-)</th>
<th>Marginal (D)</th>
<th>Failure (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Coursework</td>
<td>Questions and hands-on exercises to assess the students' understanding of the different types of software, web application, network and system attacks, and related defences. Students are required to generate reports to summarize their findings.</td>
<td>High</td>
<td>Significant</td>
<td>Moderate</td>
<td>Basic</td>
<td>Not even reaching marginal levels</td>
</tr>
<tr>
<td>2. Examination</td>
<td>The exam will include questions to assess the student’s ability to explain how various attacks work, the understanding of the principles, techniques and technologies used for defending against various attacks, and the ability to identify and discuss selected issues in computer security.</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.)
   
   The syllabus will evolve over time as current topics change. The following are example keyword syllabus: Cryptographic tools and their usage in practical settings; OS security, file system protection, access control; Identity and credential management; Memory safety, program control hijacking and defence, malicious codes, virus; network security; probing tools; Evaluating system security, secure computing platforms; cloud security; database security; Mobile security.

   Syllabus
   
   1. Selected topics in computer security:
      - Cryptographic tools and their usage in practical settings
      - Identity and credential management.
      - File system protection, access control
   
   2. Software security
      - Software attacks and countermeasures
      - web application attacks and countermeasures
   
   3. Network Security
      - Network attacks and countermeasures
      - Phases in launching an attack and countermeasures
   
   4. Other emerging topics:
      - Cloud security
      - Mobile Security
      - Database security

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.)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>