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:	Topics on Information Security
Course Code:	CS5293
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)*	CS5285 Information Security for eCommerce or equivalent
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. Abstract

This course aims at providing students with a solid understanding of a range of topics in the area of information security, with emphasis on identification of security threats to actual systems and the appropriate countermeasures. On completion of the course students should be able to 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.)

No.	CILOs	Weighting (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Identify and analyze common threats and vulnerabilities of software and web applications.	25%	✓	✓	✓
2.	Classify and analyze common threats and vulnerabilities of network and systems.	20%	✓	✓	
3.	Suggest and evaluate major countermeasures to software and web application, network and system attacks.	25%	✓	✓	✓
4.	Identify and enquire current issues in computer security.	30%	✓	✓	✓
		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	
Lectures	The different types of attacks to software, web applications, network and system 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.	✓	✓	✓	✓	
Tutorials	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.	✓	✓	✓	✓	
Project	Students will be asked to conduct a substantial case study or in-depth survey on selected security topics, such as thoroughly analysing the security properties of crypto techniques in some system/network protocols, modern encryption based access control, passwords and related usages, memory safety issues and defences, web tracking, command injection attacks and defences, cloud security, etc.	✓	✓	✓	✓	

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: 50%						
Assignment 1	25%	25%	20%	30%	7.5%	
Assignment 2	15%	15%	40%	30%	7.5%	
Quiz	30%	20%	20%	30%	15%	
Project	25%	25%	25%	25%	20%	
Examination^: 50% (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)
Problem set, including assignments, quiz, and examination	Ability to answer fundamental network/information security attacks and defences.	High	Significant	Moderate	Basic	Below Marginal
Hands-on exercises	Capacity to explore open-source security toolkit and perform hands-on exercises, as well as explore the attack and defense technologies on software, system, and web.	High	Significant	Moderate	Basic	Below Marginal
Project	Ability to conduct a substantial case study or in-depth survey on selected security topics.	High	Significant	Moderate	Basic	Below Marginal

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. Current topics will be selected from following. 1) Software security: Cryptographic toolkit with correct parameter settings in practice, memory safety, software attacks and countermeasures. 2) Web security: web application attacks and countermeasures, isolation and same origin policy, command injection identification, and defense. 3) Network Security: network attacks and countermeasures, intrusion detection systems, phases in launching an attack and countermeasures. 4) Other topics in computer security: cloud security, security policy, information governance, information privacy, security evaluation, legal issues, computer crime and computer forensics, new access control paradigms, 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.)

1.	M. Goodrich and R. Tamassia. Introduction to Computer Security. Pearson. (2014)
2.	W. Stallings and L. Brown. Computer Security: Principles and Practice. (2015)
3.	Shah S. Web 2.0 security: Defending Ajax, RIA, and SOA. Thomson (2008)
4.	Spitzner L. Honeypot: Tracking hackers. Addison-Wesley (2003)
5.	Bace R. G. Intrusion Detection. Macmillan Technical (2000)
6.	Whittaker and Thompson. How to break software security. Addison Wesley (2004)
7.	Andrews and Whittaker. How to break web software. Addison Wesley (2006)
8.	Skoudis and Liston, Counter Hack Reloaded (2e). Prentice Hall (2006)