Form 2B

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: Topics on Information Security

Course Code: CS5293

Course Duration: One Semester

Credit Units: 3

Level: P5

Medium of Instruction: English

Prerequisites: Nil

Precursors: CS5285 Information Security for eCommerce or equivalent

Equivalent Courses: Nil

Exclusive Courses: Nil

Part II

Course Aims

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.

Course Intended Learning Outcomes (CILOs)

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

No.	CILOs	Weighting (if applicable)
1.	identify and analyze common threats and vulnerabilities of software and web applications;	
2.	classify and analyze common threats and vulnerabilities of network and systems;	
3.	suggest and evaluate major countermeasures to software and web application, network and system attacks;	
4.	identify and enquire current issues in computer security.	

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.

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.

Based on the course ILOs, the teaching/learning activities of the course may include:

CILO No.	TLAs	Hours/week (if applicable)
CILO 1 – CILO 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.	
CILO 1 – CILO 4	**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. This helps support Course ILO #1, #2, #3 and #4.	
CILO 1 – CILO 4	**Case Study:** 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.	

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)

The course ILOs are accessed using the following approach:

CILO No.	Type of Assessment Tasks/Activities	Weighting (if applicable)	Remarks
CILO 1	Identify and analyze common threats and vulnerabilities of software and web applications. **Coursework:** The assignment and quizzes will include questions to assess the students' understanding of the different types of software and web application attacks. **Exam:** The exam will include questions to assess the student's understanding in how the various attacks work.		
CILO 2	Classify and analyze common threats and vulnerabilities of network and systems. **Coursework:** The assignment and quizzes will include questions to assess the students'		

	understanding of the different types of network and system attacks. **Exam:** The exam will include questions to assess the ability of the students to explain how the various attacks work.		
CILO 3	Suggest and evaluate major countermeasures to software and web application, network and system attacks. **Coursework:** The assignment and quizzes will include questions to assess the students' understanding of the different types of technologies used for defending against software and web application attacks, network and system attacks. **Exam:** The exam will include questions to assess the students' understanding of the principles, techniques and technologies used for defending against various attacks.		
CILO 4	Identify and enquire current issues in computer security. **Coursework:** Students may be required to complete a report on a selected topic. In the information gathering and research process, students are required to identify and discuss the current issues in computer security. The quality and relevance of their research findings will be a measure for this ILO. **Exam:** The exam will include questions to assess students' ability to identify and discuss selected issues in computer security.		

Grading of Student Achievement:

Examination duration: 2 hours

Percentage of coursework, examination, etc.: 30% CW; 70% 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

The syllabus will evolve over time as current topics change. The following are example keyword syllabus: Security policies and legal issues; hardware security, OS security, file system protection, access control; Cryptographic tools; Identity and credential management, security administration; Hacking attacks and countermeasures, probing tools, malicious codes, virus, security administration; Evaluating system security, TCSEC, CC, secure computing platforms; programming for security, security development process; Database security; Incident and Intrusion handling; Mobile security.

Syllabus

Topics will be selected from following:

1. Software security
    - Software attacks and countermeasures
    - web application attacks and countermeasures
    - web 2.0 application attacks and countermeasures

2. Network Security
    - Network attacks and countermeasures
    - Intrusion detection systems
    - Phases in launching an attack and countermeasures

3. Selected topics in computer security
    - Security policy, Information Governance, Information Privacy, Security Evaluation, Legal issues, Computer Crime and Computer Forensics, New Access Control Paradigms, Mobile Security, Database security

Recommended Reading
Text(s)

Essential Text

Whittaker and Thompson. How to break software security. Addison Wesley (2004)

Andrews and Whittaker. How to break web software. Addison Wesley (2006)

Skoudis and Liston, Counter Hack Reloaded (2e). Prentice Hall (2006)

Supplementary Reading

Shah S. Web 2.0 security: Defending Ajax, RIA, and SOA. Thomson (2008)

Spitzner L. Honeypot: Tracking hackers. Addison-Wesley (2003)

Bace R. G. Intrusion Detection. Macmillan Technical (2000)

Online Resources