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: Network and Information Security

Course Code: CS6287

Course Duration: One Semester

Credit Units: 3

Level: P6

Medium of Instruction: English

Prerequisites:
CS5222 Computer Networks and Internets or
EE5412 Telecommunication Networks or equivalent

Precursors: Nil

Equivalent Courses: Nil

Exclusive Courses:
For MSc Computer Science and MSc Electronic Commerce programmes, CS6287 Network and Information Security is exclusive with CS5285 Information Security for eCommerce.

Part II

Course Aims

This course is aimed at developing understanding and skill in protecting networks from external attack and internal misuse. Techniques to ensure information security in its storage, transfer and reception are also dealt with, including principles of encryption schemes, their properties and applications to security protocols. Authentication protocols and various trust models are analyzed. E-Commerce protocols such as secure payment protocols are also studied. Students should be able to design and evaluate provisions for network security and set up secure web-based services. He/she should also be able to make technical choices on encryption-based systems and use them to secure transactions over open network.

Course Intended Learning Outcomes (CILOs)

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

No.	CILOs	Weighting (if applicable)
1.	identify and justify security requirements on data storage, communication, and transactions;	15%
2.	apply basic network protection techniques;	25%
3.	describe relevant properties of cryptographic schemes and apply them in the design of security protocols;	30%
4.	apply basic countermeasures to protect against attacks on common web applications, and critique on their adequacies.	30%

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.

CILO No.	TLAs	Hours/week (if applicable)
CILO 1	Knowledge and skill for this CILO will be explained in lectures. Tutorial exercises and discussion will help the students to attain this CILO.	
CILO 2	Knowledge and skill for this CILO will be explained in lectures. Tutorial exercises and discussion will help the students to attain this CILO. Further reading on common cases will be given.	
CILO 3	Common cryptographic schemes will be explained in lectures with emphasis on the properties that will be used in the design of security protocols. Tutorial exercise and discussions will be used to help students understanding and skill in apply the techniques taught. A cryptographic package will be used to provide practical hands-on experience in the Lab.	

CILO 4	Basic principles and examples will be explained in lectures and tutorials. Tutorial exercises and discussions on cases will further help student attain this CILO. Students are required to critique on the adequacies of countermeasure schemes.	

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)

CILO No.	Type of Assessment Tasks/Activities	Weighting (if applicable)	Remarks
CILO 1	Tutorial exercises, assignments, quiz, exam		
CILO 2	Tutorial exercises, assignments, quiz, exam		
CILO 3	Assignments, quiz, exam, exercise on practical hands-on on cryptographic package and use of public key encryption scheme		
CILO 4	Tutorial exercises, assignments, quiz, exam		

Grading of Student Achievement: Refer to Grading of Courses in the Academic Regulations for Taught Postgraduate Degrees.

Examination duration: 2 hours

Percentage of coursework, examination, etc.: 40% CW; 60% 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

Security requirements and policy, Security Attacks, Network access control, Firewalls, Application proxies, Intrusion detection, operating system security, Authentication factors, Authentication protocols, Web security and privacy, Email security, Encryption algorithms, Secret key, Public key, Digital signature, Certificate authority, Public key infrastructure, Trust model; Transport and Network level security, SSL, TLS, IPSec, VPN, Payment protocols, Secure electronic transaction, Electronic voting, Digital money, Wireless security, Digital watermarks.

Recommended Reading
Text(s)

W Stalling, Cryptography and Network Security: Principles and Practice, 5th edition, by, Prentice Hall 2010

C Kaufman, R Perlman, M Speciner, Network Security, 2nd edition, by, Prentice Hall 2002

Online Resources

Up-to date online resources will be given.