City University of Hong Kong

Information on a Course
offered by Department of Electronic Engineering
with effect from Semester A 2012/13

Part I

Course Title:	Topics in Security Technology
Course Code:	EE5815
Course Duration:	One Semester (13 weeks)
No. of credits:	3
Level:	P5
Medium of Instruction:	English
Prerequisites:	Nil
Precursors:	MA3150 Advanced Mathematical Analysis; or MA3151 Advanced Engineering Mathematics
Equivalent Course:	Nil
Exclusive Courses:	Nil

Part II

Course Aims:

This course aims to provide students with an understanding of the principles of computer security technologies, including the principles of cryptography, side channel attacks and securities for data, communications, cloud computing and smart cards.

Course Intended Learning Outcomes (CILOs)

No.	CILOs
1.	Identify the conceptual difference between threats, vulnerabilities and attack.
2.	Recognize techniques and mechanisms for safeguarding an attack.
3.	Identify the use of preventive and logistic techniques for safeguarding a computer system.
4.	Describe the current techniques and anticipated trends in Internet security development, cloud computing security.
5.	Analyse and explain various security issues in different card & Internet technologies.

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)

Timetabling Information

Pattern	Hours
Lecture:	*24*
Tutorials:	*12**
Laboratory:	*3*
Other activities:	

** Some of the tutorials will be conducted in the laboratory.*

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)

	Type of assessment tasks	*Weighting (if applicable)*
Continuous Assessment	Assignments and Quizzes	40%
Examination	Written exam	60% 2 hours

Remarks:. To pass the course, students are required to achieve at least 35% in course work and 35% in the examination. Also, 75% laboratory attendance rate must be obtained.

Grading of Student Achievement:

Letter Grade	Grade Point	Grade Definitions
A+ A A-	4.3 4.0 3.7	Excellent
B+ B B-	3.3 3.0 2.7	Good
C+ C C-	2.3 2.0 1.7	Adequate
D	1.0	Marginal
F	0.0	Failure

Constructive Alignment with Programme Outcomes

PILO	How the course contribute to the specific PILO(s)
1	An ability to apply knowledge of engineering is appropriate to the degree discipline. Students will learn security techniques for enhancing the safety of computer, network and portable devices and apply these techniques to the solution of engineering problems in class.

2	An ability to design and conduct experiments as well as to analyze and interpret data is appropriate to the degree discipline. Students will learn the programming techniques for smart card and analyze new security technologies.
3	An ability to design a system, component, or process that conforms to a given specification within realistic constraints is appropriate to the degree discipline. Students will learn design a security system and learn the technique to analysis the risk of the designed system. They are required to work with the constraints specified in the environment including components, interconnectivity and network link.
4	An ability to evaluate and formulate solutions to system security problems effectively and responsibly as a team member is appropriate to the degree discipline. Students will work in groups of 2 and split the work in amongst them and coordinate the design into a workable system.
5	An ability to conduct some research, identify, formulate and solve engineering problems is appropriate to the degree discipline. Students will integrate the smart card device and design appropriate software to solve the design/implementation/integration problems.
6	An ability to communicate effectively is appropriate to the degree discipline. Students work in groups and they will practice the skill to communicate with each other to prepare the formal laboratory report.
7	An ability to learn how to manage a team of technologists using necessary engineering tools is appropriate to the degree discipline. Students will be given a chance to present their work in class and collect feedbacks from other students.

Part III

Keyword Syllabus:

Threats to Computer Systems
Threats, Vulnerabilities and Attacks, System security Engineering, Threat trees, Categorization of Attacks, Trojan Horse and Viruses, Common Attack Methods.

Preventive Security Approaches
Auditing and Intrusion Detection, Identification and Authentication and Encryption.

Logistic Security Approaches
Key Management protocols -, Access Control, Convert Channels, Composing Security, Privileges and Roles, Security Kernel.

Computer Security Applications
Network Security Methods, Data Base Security Methods, Trusted Network Interpretations, WIFI and P2P security, cloud computing security.

Card Security Applications
Smart Card ISO standards, Security Methods – encryption, key management and access control.

Recommended Reading:

Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems (Wiley; 2 edition (April 14, 2008), ISBN-10: 0470068523)

William Stalling, Lawrie Brown, Computer Security: Principles and Practice (Prentice Hall, 2008, ISBN 0-13-600424-5)

William Stalling, Cryptography and Network Security (Prentice Hall, 2006, ISBN 0-13- 187316-4)

E. Amoroso: Cyber Security (Silicon Press, 2006, ISBN 0929306384)

Matt Bishop, Introduction to Computer Security (Addison-Wesley Professional, 2005, ISBN 0-32-124744-

E. Amoroso: Fundamentals of Computer Security Technology (Prentice Hall, 1994, ISBN 0-13-108929-1)

J.A. Cooper: Computer and Communications Security (McGraw Hill, 1989, ISBN0-07-012926-6)

S.Muffic: Security Mechanisms for Computer Networks (John Wiley &Sons, 1989, ISBN 0-470-21387-6)

J.B. Grimson & H.J. Kugler: Computer Security: the practical issues in a troubled world (North Holland 1985, ISBN 0-444-87801-7)

Online Resources (if any)

http://csrc.nist.gov/publications/drafts/800-124/Draft-SP800-124.pdf, DRAFT Guidelines on Cell Phone and PDA Security (National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, SP 800-124, Jul 2008)

http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf, An Introduction to Computer Security: The NIST Handbook (National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, SP 800-12, Oct 1995)