THE CHINESE UNIVERSITY OF HONG KONG
Print Course Catalog Details

Academic Org: Div of Computer Science & Engg – Subject: Courses offered by Fac of Erg

Course: ENGG5105 **Course ID:** 011158 **Eff Date:** 2022-07-01 **Crse Status: Active** **Apprv. Status:** Approved **[**Course Rev**]**

Computer and Network Security **電腦系統與網絡安全**

This course aims to introduce important topics in computer and network security from an applied perspective. Topics include: (i) applied cryptography (e.g., cryptographic primitives, programming with OpenSSL), (ii) network security (e.g., unauthorized accesses, large-scale network attacks, firewall & intrusion detection systems), (iii) web security (e.g., HTTP session management and web attacks), and (iv) system security (e.g., buffer overflow, passwords, file system security). The course also discusses latest applied security topics depending on the current research trends.
Advisory: Students are expected to have taken CSCI3150 or ESTR3102, and CSCI4430 or CENG4430 or IERG3310

本科旨在從應用角度介紹有關計算機和網絡安全的重要課題。主題包括：（一）應用密碼學（如密碼學原型、OpenSSL編程），（二）網絡安全（如未經授權訪問、大規模網絡攻擊、防火牆和入侵檢測系統），（三）萬維網安全（如HTTP連接管理和萬維網攻擊），（四）系統安全（如緩衝溢出、密碼、檔案系統的安全性)。本科也會按目前研究趨勢討論最新的應用安全課題。
建議：學生應曾修讀CSCI3150或ESTR3102，及CSCI4430或CENG4430或IERG3310。

Grade Descriptor:

A

EXCELLENT – exceptionally good performance and far exceeding expectation in all or most of the course learning outcomes; demonstration of superior understanding of the subject matter, the ability to analyze problems and apply extensive knowledge, and skillful use of concepts and materials to derive proper solutions.

有關等級說明的資料，請參閱英文版本。

B+

B

GOOD – good performance in all course learning outcomes and exceeding expectation in some of them; demonstration of good understanding of the subject matter and the ability to use proper concepts and materials to solve most of the problems encountered.

有關等級說明的資料，請參閱英文版本。

C

FAIR – adequate performance and meeting expectation in all course learning outcomes; demonstration of adequate understanding of the subject matter and the ability to solve simple problems.

有關等級說明的資料，請參閱英文版本。

D

MARGINAL – performance barely meets the expectation in the essential course learning outcomes; demonstration of partial understanding of the subject matter and the ability to solve simple problems.

有關等級說明的資料，請參閱英文版本。

F

FAILURE – performance does not meet the expectation in the essential course learning outcomes; demonstration of serious deficiencies and the need to retake the course.

有關等級說明的資料，請參閱英文版本。

Equivalent Offering:
Units: 3 (Min) / 3 (Max) / 3 (Acad Progress)
Grading Basis: Graded
Repeat for Credit: N
Multiple Enroll: N
Course Attributes: MSc Computer Science
MPhil-PhD Computer Sci & Erg

MPhil-PhD Electronic Erg
MPhil-PhD Info Engineering
MPhil-PhD Mechan & Auto Erg
MPhil-PhD System Erg & Erg Mgt
MPhil-PhD Information Engineering
MPhil-PhD Biomedical Engineering

Topics:

COURSE OUTCOMES

Learning Outcomes:

At the end of the course of studies, students will have acquired the ability to
1. identify programs that are vulnerable to buffer overflow attacks.
2. analyse network logs to identify network-related attacks based on IP spoofing, TCP exploit, arp-spoofing, and man-in-the-middle attacks.
3. set up a firewall properly.
4. protect information based on encryptions and authentications.

Course Syllabus:

This course aims to introduce important topics in computer and network security from an applied perspective. Topics include: (i) applied cryptography (e.g., cryptographic primitives, programming with OpenSSL), (ii) network security (e.g., unauthorized accesses, large-scale network attacks, firewall & intrusion detection systems), (iii) web security (e.g., HTTP session management and web attacks), and (iv) system security (e.g., buffer overflow, passwords, file system security). The course also discusses latest applied security topics depending on the current research trends.

Assessment Type:

Essay test or exam	: 50%
Others	: 50%

Feedback for Evaluation:

1. Quiz and examinations
2. Course evaluation and questionnaire
3. Question-and-answer sessions during class
4. Student consultation during office hours or online

Required Readings:

To be provided by course teacher.

Recommended Readings:

1. Aleph One, "Smashing the Stack for Fun and Profit", Phrack 49, Volume Seven, Issue Forty-Nine, File 14 of 16, 1996.
2. Scott Fluhrer, Itsik Mantin, and Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", 8th Annual Workshop on Selected Areas in cryptography, 2001.
3. Brecht Claerhout, "A short overview of IP spoofing: Part I", This paper can be found in many web archives, but does not seem to be published formally, 2001.
4. Charlie Kaufman, Radia Perlman and Mike Speciner. "Network Security - Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002
5. Ed Skoudis and Tom Liston, "Counter Hack Reloaded", 2nd edition, Prentice Hall, 2010
6. William Stallings, "Cryptography and Network Security", 5th Edition, Prentice Hall, 2010

OFFERINGS

1. ENGG5105 — Acad Organization=CSEGV; Acad Career=RPG

COMPONENTS

LEC : Size=30; Final Exam=Y; Contact=3
TUT : Size=30; Final Exam=N; Contact=1

ENROLMENT REQUIREMENTS

1. ENGG5105

Enrollment Requirement Group:
For students in MSc Computer Science or MPhil-PhD programmes under Faculty of Engineering or UG Computer Science or UG Computer Engineering;
Not for students who have taken CMSC5726 or CSCI5470

CAF