Course: ENGG5105  
Course ID: 011158  
Eff Date: 2024-07-01  
Crse Status: Active  
Apprv. Status: Approved  

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

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.
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%
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:
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.

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
### Additional Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VTL-Onsite face-to-face hrs</td>
<td>0</td>
</tr>
<tr>
<td>VTL-Online synch. hrs</td>
<td>0</td>
</tr>
<tr>
<td>VTL-Online asynch. hrs</td>
<td>0</td>
</tr>
</tbody>
</table>

<END OF REPORT>