Course Code: CSIT5740
Course Title: Introduction to Software Security (3 units)

Name: Dr. Alex LAM
Email: lamngok@cse.ust.hk

Core elements:

i. Course description;

This course serves as an introduction to the concept of software security. The students will learn fundamental concepts on software security, security mechanisms in software and operating systems, secure coding guidelines and exploits, and advanced analysis techniques for security. Students will also have hands-on experience in deploying security attacks and analysis of real world security vulnerabilities.

ii. Course learning outcomes;

On successful completion of the course, students will be able to:

1. Identify and explain the major threats in software security.
2. Explain the corresponding mitigation methods for common software security attacks.
3. Get familiar with practical tools and methods for the analysis of software vulnerabilities.
4. Perform both attack and defense on real-world software systems.

iii. List of assessment tasks with weightings;

1. Two homework assignments (2x7.5%= 15% of the grade)
2. Midterm exam (25% of the grade)
3. Final exam (60% of the grade)

iv. Mapping against course learning outcomes; and,

Assessment Method	weight	CILOs to be addressed
Homework assignments	15%	1, 2, 3, 4
Midterm exam	25%	1, 2, 4
Final exam	60%	1, 2, 4

v. Week-by-week content (subject to changes)

Week number	Content (tentative, subject to the actual teaching progress)
1	**Introduction to software security threats with real-world examples**
2	**The software threat model, introduction to the Linux security measures, introduction to the Kali penetration testing platform**
3	**Holiday**
4	**The Linux security measures, simple attacks on Linux systems**

5	**Assembly preliminaries, introduction to x86 instruction set, function calls**
6	**Function call examples, introduction to memory vulnerabilities, memory exploitations**
7	**Memory exploitations, shell coding, overflow attacks, other forms of attacks**
8	**Mechanisms to mitigate memory vulnerabilities**
9	**Midterm exam**
10	**Introduction to Web security**
11	**The same origin policy, cookies, introduction to web attacks**
12	**Introduction to web attacks**
13	**Web injection attacks**

Academic Integrity

Students are expected to adhere to the university's academic integrity policy. Students are expected to uphold HKUST's Academic Honor Code and to maintain the highest standards of academic integrity. The University has zero tolerance of academic misconduct. Please refer to Academic Integrity | HKUST – Academic Registry for the University's definition of plagiarism and ways to avoid cheating and plagiarism.

Optional elements:
i. Instructor office hours and consultations;
ii. Final grade description;
iii. Level of programming expected; and,
iv. Whether the course includes a group project.