The Hong Kong University of Science and Technology

UG Course Syllabus (Spring 2025-26)

[Course Title] Competitive Programming in Cybersecurity II

[Course Code] COMP 3633

[No. of Credits] 2-credit

[Any pre-/co-requisites] Prerequisite(s): COMP 2633

Name: Dr. LAM Ngok

Email: lamngok@cse.ust.hk

Course Description

This is the second course out of a series of three special courses that aim to prepare interested students in joining the various cybersecurity competitions. The topics discussed will be practical and related to the cybersecurity competitions.

Intended Learning Outcomes (ILOs)

By the end of this course, students should be able to:

1. apply and understand ethical hacking.
2. analyse various computer systems rigorously and identify potential security flaws in the systems.
3. understand the current trends in the development of cybersecurity protection measures in the industry.
4. acquire leadership through team-working in taking part in the cybersecurity contests.
5. educate less experienced students regarding cybersecurity and provide the leadership in sharing and deepening the understanding of cybersecurity issues among the student community.

Assessment and Grading

This course will be assessed using criterion-referencing and grades will not be assigned using a curve. Detailed rubrics for each assignment are provided below, outlining the criteria used for evaluation.

Assessments:

Assessment Task	Contribution to Overall Course grade (%)	Due date
New hacking technique presentation	50%	Before the end of the semester
Course participation	15%	Before the end of the semester
International CTF competition and technical participation	35%	Before the end of the semester

Grading Rubrics

Mapping of Course ILOs to Assessment Tasks

Assessed Task	Mapped ILOs	Explanation
New hacking technique presentation	ILO1, ILO2, ILO3. ILO4, ILO5	This task assesses students' ability to learn themselves and teach others the new hacking techniques. This task will be delivered with a heavy emphasis on ethical hacking.
Course participation	ILO1, ILO3, ILO4	This task assesses students' ability to collaborate with other students
International CTF competition and technical participation	ILO1, ILO2, ILO3. ILO4, ILO5	This task assesses students' ability to apply hacking techniques to compete in international competitions. This task has a heavy emphasis on the technical skills learned, team-working and also on ethical hacking.

Grading Rubrics

Final Grade Descriptors:

Grades	Short Description	Elaboration on subject grading description
A	Excellent Performance	Demonstrates a comprehensive grasp of ILO1-ILO5
B	Good Performance	Shows good knowledge and understanding of the main contents in ILO1-ILO5
C	Satisfactory Performance	Possesses adequate knowledge of the contents in ILO1-ILO5
D	Marginal Pass	Has threshold knowledge of the contents in ILO1-ILO5
F	Fail	Demonstrates insufficient understanding of the subject matter.

Course AI Policy

This course does not allow using generative artificial intelligence tools to complete the assessment tasks.

Communication and Feedback

Assessment marks for individual assessed tasks will be communicated via email at the end of the semester

Resubmission Policy

NA

Required Texts and Materials

N/A

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.

Additional Resources

N/A

List of Presentation Topics (subject to change from semester to semester):

Pwn	**Crypto**	**Reverse**	**Web**	**Misc**
Ret2dl_resolve	Lattice-based attack for RSA	RE Automation	NAT slipstream	Cryptocurrency Security
FSOP	Bleichenbacher & Manger attacks	Self written RE tools / project / plugins	Request smuggling	Windows Active Directory / Azure AD Attack
House of Force	Common attack vectors for Elliptic curve cryptology	Reversing a specific modern language (e.g. compiled language features of Rust / Go / Kotlin in JVM / Swift / various mobile frameworks etc)	JavaScript prototype pollution	Memory Forensics / How to find interesting info from memory?
Unsortbin attack + Global_max_fast Hijacking	Study of one major postquantum cryptography type: code-based, lattice-based, hash-based, multivariate	Packing and Unpacking binaries	NoSQL Injections	Container and Cloud Security (e.g. docker / kubernetes internals, AWS / Azure security)

Introduction to Kernel exploitation	Study of implementation flaws of major crypto libraries	Advanced Angr	DNS Rebinding	Advanced OSINT / Threat Intelligence Technique
Sandbox escape		APT malware reverse engineering (eg compiler-level obfuscations) (Links to an external site.)	OAuth	Hardware side channels (Rowhammer, CPU side channels, cache attacks etc)
Windows Pwn			GraphQL	Any techniques / knowledge that you found interesting from MITRE ATT&CK table
House of orange (challenger level)			Java deserialization	Discussion of recent cybersecurity incidents - technical side
			Expression Language Injection	Introduction to fuzzing (eg AFL, honggfuzz, libfuzzer,etc)
			UXSS (should be in pwn?)	Summary of any Brandon Falk 's live streaming gamozolabs
				CodeQL tutorial
				Walkthrough of any Nday exploit chain being used in the wild