The Hong Kong University of Science and Technology

UG Course Syllabus (Fall 2025-26)

[Course Title] Cybersecurity

[Course Code] COMP 4634

[No. of Credits] 3

[Pre-/co-requisites] COMP 3631: Cryptography

Name: SHE Dongdong

Email: dongdong@cse.ust.hk

Course Description

Based on 3631 Cryptography, this course is an introduction to the theory and application of cybersecurity. Cybersecurity, also called computer security or IT security, refers to the study of techniques to protect computing systems from attacks that threaten data confidentiality, system integrity and availability. By modeling, analyzing, and evaluating the security of computer systems, students will learn to find weaknesses in software, hardware, networks, data storage systems, mobile applications, and the Internet, and identify current security practices and defenses to protect these systems.

List of Topics

Topic
Introduction; Security Mindset
Cryptography Recap
Reverse Engineering
Malware
Software Exploitation: Buffer Overflow | Examples for ROP Attack.
Software Exploitation: Others
Software Protection: Obfuscation

Topic
Software Security Analysis: Dynamic Vulnerability Detection
Software Security Analysis: Static Security Analysis
Industry Perspective on Computing Security
Side Channels
Authentication: Password & Biometrics
Network Security
Authorization
Protocol
Trusted Computing
Blockchain
Smart Contract Security | Internet of Things (Short)
Machine Learning Security

Intended Learning Outcomes (ILOs)

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

- ILO1: State and describe the underpinning principles of cybersecurity and relate them to past and ongoing events
- ILO2: Apply cybersecurity principles to recognize vulnerabilities in computer systems, including protocols, hardware, and software
- ILO3: Identify and implement effective defenses for computer systems against potential cybersecurity attacks
- ILO4: Study and understand cybersecurity protections and attacks on networks, databases, financial systems and operating systems
- ILO5: Understand how to design and apply business continuity plans, incidence response plans, and cybersecurity risk analysis to enforce cybersecurity best practices in business

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
Assignment 1	10%	23/09/2025 *
Assignment 2	10%	23/10/2025 *
Assignment 3	10%	23/11/2025 *
Course Project	20%	10/12/2025 *
Midterm Exam	25%	22/10/2025 *
Final Exam	25%	10/12/2025 *

* Assessment marks for individual assessed tasks will be released within two weeks of the due date.

Mapping of Course ILOs to Assessment Tasks

Assessed Task	Mapped ILOs	Explanation
Assignment 1	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' ability to state and describe principles of cybersecurity (ILO 1), apply it to recognize vulnerabilities (ILO 2), implement effective defenses (ILO 3), understand cybersecurity protections and attacks (ILO 4), and design business continuity plans (ILO 5).
Assignment 2	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' ability to state and describe principles of cybersecurity (ILO 1), apply it to recognize vulnerabilities (ILO 2), implement effective defenses (ILO 3), understand cybersecurity protections and attacks (ILO 4), and design business continuity plans (ILO 5).
Assignment 3	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' ability to state and describe principles of cybersecurity (ILO 1), apply it to recognize vulnerabilities (ILO 2), implement effective defenses (ILO 3), understand cybersecurity protections and attacks (ILO 4), and design business continuity plans (ILO 5).
Course Project	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' comprehensive cybersecurity capabilities, beginning with their

		ability to articulate core principles (ILO 1). It evaluates their practical skills in applying these principles to recognize system vulnerabilities (ILO 2), implement effective defenses (ILO 3), and analyze various protections and attacks (ILO 4). Finally, it measures their strategic competence in designing essential business continuity plans (ILO 5)."
Midterm Exam	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' ability to apply foundational cybersecurity principles (ILO 1) to recognize vulnerabilities (ILO 2), implement defenses (ILO 3), analyze threats (ILO 4), and design strategic business continuity plans (ILO 5).
Final Exam	ILO1, ILO2, ILO3, ILO4, ILO5	This task assesses students' ability to apply foundational cybersecurity principles (ILO 1) to recognize vulnerabilities (ILO 2), implement defenses (ILO 3), analyze threats (ILO 4), and design strategic business continuity plans (ILO 5).

Grading Rubrics

Detailed rubrics for each assignment will be provided. These rubrics clearly outline the criteria used for evaluation. Students can refer to these rubrics to understand how their work will be assessed.

Final Grade Descriptors:

Grades	Short Description	Elaboration on subject grading description
A	Excellent Performance	Demonstrates a comprehensive grasp of subject matter, expertise in problem-solving, and significant creativity in thinking. Exhibits a high capacity for scholarship and collaboration, going beyond core requirements to achieve learning goals.
B	Good Performance	Shows good knowledge and understanding of the main subject matter, competence in problem-solving, and the ability to analyze and evaluate issues. Displays high motivation to learn and the ability to work effectively with others.
C	Satisfactory Performance	Possesses adequate knowledge of core subject matter, competence in dealing with familiar problems, and some capacity for analysis and critical thinking. Shows persistence and effort to achieve broadly defined learning goals.
D	Marginal Pass	Has threshold knowledge of core subject matter, potential to achieve key professional skills, and the ability to make basic judgments. Benefits from the course and has the potential to develop in the discipline.
F	Fail	Demonstrates insufficient understanding of the subject matter and lacks the necessary problem-solving skills. Shows limited ability to think critically or analytically and exhibits minimal effort

		towards achieving learning goals. Does not meet the threshold requirements for professional practice or development in the discipline.

Course AI Policy

In this course, students are permitted to use generative artificial intelligence (AI) tools as aids for learning and productivity. However, the responsible and transparent use of these tools is mandatory.

Permitted Uses Include:

- Brainstorming and exploring initial ideas.
- Checking grammar, spelling, and refining writing style.
- Summarizing complex texts for better understanding.
- Debugging code and suggesting optimizations.

Prohibited Uses Include:

- Generating entire essays, reports, or solutions and submitting them as your own work.
- Using AI tools during quizzes, tests, or exams.
- Representing AI-generated ideas or text as your own original thought without citation.

Communication and Feedback

Assessment marks for individual assessed tasks will be communicated via Canvas within two weeks of submission. Feedback on assignments will include specific details, such as deduction points, knowledge points that need to be mastered, and specific solutions. Students who have further questions about the feedback including marks should consult the instructor within five working days after the feedback is received.

Resubmission Policy

Extensions for assignments and arrangements for make-up exams are not guaranteed. If students face an emergency or an unavoidable conflict (such as a documented illness or required business travel), he/she must obtain the instructor's consent prior to the deadline.

Required Texts and Materials

Information Security: Principles and Practice

Introduction to Computer Security

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