

香港中文大學
CUHK

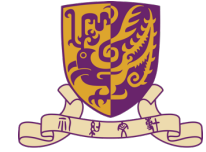
Course Overview

Yajin ZHOU

<https://yajin.org>

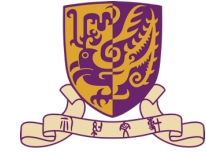
Credits: Some of the slides are from CS161 of UC Berkeley

Instructor



- Yajin Zhou (yajin@yajin.org)
- Research areas:
 - System security: how to locate vulnerabilities and how to develop efficient defense methods
 - AI security: security for AI and AI for security
 - Blockchain/Web3 security
 - Blockchain system and smart contracts
 - **Cybercrime leveraging cryptocurrencies**

Instructor

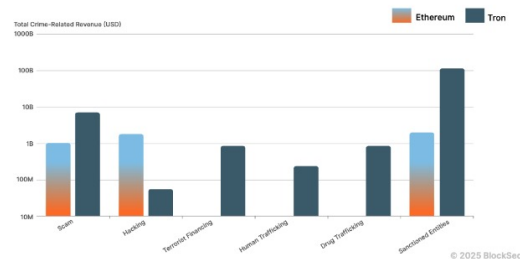


- Research areas:
- **Cybercrime leveraging cryptocurrencies**

BlockSec 2025 Crypto Crime Report

Illicit revenue by crime type — Ethereum vs TRON

► Crime-Related Revenue by Crime Type and Blockchain



Source: BlockSec 2025 Crypto Crime Report — proprietary on-chain data.

IN THE NEWS • The Record, 2025

Cambodian scam giant handled \$49 billion in crypto transactions since 2021, researchers say

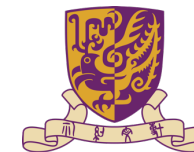
A notorious online marketplace allegedly tied to cyber scam operations and linked to the family ruling Cambodia has processed more than \$49 billion in cryptocurrency transactions since 2021, according to a new report.

US\$4B+

Laundered via Cambodia's Huione — now cut off from the US dollar system (FinCEN, 2025).

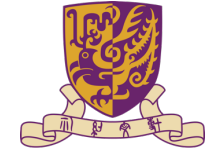
US\$1.5B

Stolen from Bybit by North Korea's Lazarus, then laundered on-chain in days (FBI, 2025).



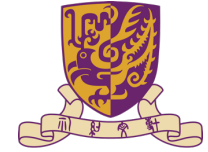
Learning Objectives

- How to think adversarially about computer systems
- Understanding common vulnerabilities
- How attacks really work in practice
- Know how build a computer system with robust security properties
- Know mistakes not to make



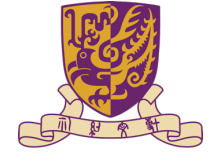
Prerequisites

- C and assembly language
- Operating systems
- Computer networking



Course Website

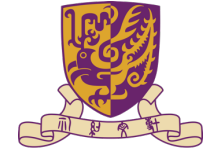
- All course logistics are available on Blackboard
 - https://blackboard.cuhk.edu.hk/ultra/courses/_267936_1/
 - <https://yajin.org/teaching/IERG4130/2026/>



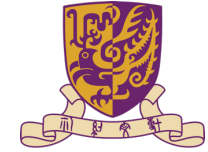
TAs & Office Hours

- CAI Jianquan: Lead TA
- CHEN Jianzhou
- SHI Luxin
- WANG Hailin
- TA's office hours are available on blackboard
- My office hour:
 - 11:20 – 12:20 on Friday or making email appointment
 - **SHB 714**

Tutorial

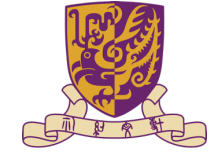


- We will have one tutorial each week
- The classroom and time are TBD



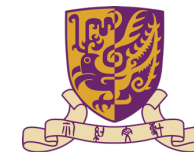
Course Structure

- We will cover the following topics
 - Basic principles
 - Software security
 - Cryptograph
 - Web security
 - Network security
 - Emerging topics: AI/Web3 security



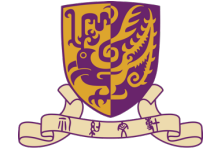
Course Assessment

- Assignments: 20
- Labs: 20
- Midterm: 15
- In-class quiz: 5
- Final Examination: 40
- Late submission policy
 - If the submission is late but within 1 calendar days after the deadline, there will be a deduction of 10% from the marks awarded for the submitted piece of work.



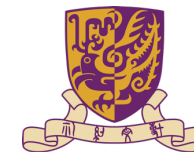
Late Submission

- Late submissions are accepted.
- For each calendar day after the deadline, 10% will be deducted from the marks awarded for the submitted work.
- Exceptions may be granted in the case of emergencies or medical circumstances, subject to the submission of appropriate supporting documentation.



Resources

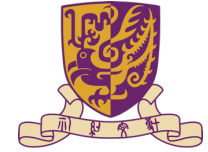
- CS161 of UC Berkeley
- CSE 443 of PSU (Trent Jaeger)
- CS-412 of EPFL (Mathias payer)
- CMPSC 447 of PSU (Gang Tan)



Resources

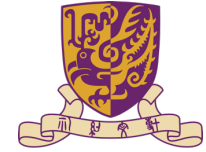
- Blackboard
 - Announcement will be on the blackboard
 - Discussion on the blackboard is highly encouraged
 - Use of AI is encouraged, **but you need to have your own judgement!**
- Email
 - Email me (yajin@ie.cuhk.edu.hk) to make appointment

Academic Integrity

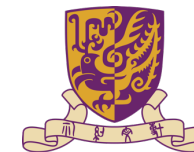


- We encourage the discussion with each other
- But do not directly copy code and answers from others!

Stress Management and Mental Health



- Your health is more important than this course
- If you feel overwhelmed or under too much stress, please reach out to me.
- You are welcome to set up a meeting with me, and we can work out a study plan together.
- If you find the course too challenging or feel that it may not be the right fit for you, dropping the course early is another option: it is better to make that decision early than to struggle throughout the semester.



Ethical Issue

- This class may contain technologies whose abuse may infringe on rights of others!
- It is usually okay to break into your own systems
- It is usually okay to break into someone else's systems with their explicit permission
- It is unethical and exceedingly **criminal** to break into someone else's systems **without** their permission