CSIT5730: Principles of Cybersecurity (Fall 2024)

Schedule | Grading | Policies | Canvas

Instructor	Shuai Wang (shuaiw@cse.ust.hk)
Time/Location	Thu 19:30 – 22:20, 2464.
TA	Sen DENG (sdengan@cse.ust.hk)
Textbook (NOT required; E-book is fine.)	Information Security: Principles and Practice By Mark Stamp. Second edition. Addison-Wesley. 2011. Introduction to Computer Security. By Michael T Goodrich and Roberto Tamassia. First edition. Addison-Wesley. 2013.
In-class Mid. Exam	10/10; lecture time (100 mins).
Final Exam	TBA

Class Description

This course provides an introduction to the theory and application of cybersecurity. Students will develop the skills necessary to formulate and address the security needs of real-world environments. The topics of this course include cryptographic models and methods, software security, system security, network security, and conclude with emerging trends in cybersecurity.

Expected Work

Students are required to attend all lectures, read all required textbook chapters and additional reading materials, complete the assignments on time, and take the in-class quizzes, midterm and final exams.

Assignments have to be complete by the student individually and submitted through Canvas.

Class Schedule

Below is the calendar for this semester course. This is the preliminary schedule, which will be altered as the semester progresses. It is the responsibility of the students to frequently check this web-page for schedule, readings, and assignment changes. As the professor, I will attempt to announce any change to the class, but this web-page should be viewed as authoritative. If you have any questions, please contact me.

Date	Topic	Readings/Notes/Homework	Misc.
05/09	Introduction; Security Mindset | Slides | Classic Crypto | Slides	A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles. link. notes	
12/09	Symmetric Key Crypto | Slides	Stream Ciphers: Dead or Alive? link. Chapter 2; 3 of the first textbook. Limitations of the Even-Mansour Construction Introduction to Authenticated Encryption. link. notes	HW1 release
19/09	Public Key Crypto | Slides	Chapter 4 and 5 of the first textbook. Notes RSA Correctness Proof	
26/09	Software Security (Reverse Engineering and Malware) | Slides	Towards Reverse-Engineering Black-Box Neural Networks Link. Hacking the Xbox Link. notes Reflections on Trusting Trust Link. Chapter 11 of the first textbook.	
03/10	Software Security (Exploitation and Protection) | Slides	Smashing The Stack For Fun And Profit Link. SoK: Automated Software Diversity Link.	HW2 release

Date	Topic	Readings/Notes/Homework	Misc.
10/10	In-class mid-term (first 100 minutes) | Group Project Clarification.	Notes Chapter 11 of the first textbook.	Location: TBA
17/10	Software and System Security (Dynamic and Static Vulnerability Detection)	The Art, Science, and Engineering of Fuzzing: A Survey Link. The Fuzzing Book Link. Certification of Programs for Secure Information Flow Link.	
24/10	Advanced Software and System Security Topics (Exploitations and Side Channel) | Slides	Notes About Directed Fuzzing and Use-After-Free: How to Find Complex & Silent Bugs? A practical implementation of the timing attack Link. FLUSH+RELOAD Link. Recovering images paper	
31/10	Authentication and Network Security | Slides	Note Chatper 7 and Appendix A-1 of the first textbook.	
07/11	Authorization and Protocols | Slides	Section 8.9 8.10, 9 of the first textbook.	HW3 release
14/11	Blockchain and Smart Contract | Slides	Bitcoin: A peer-to-peer electronic cash system Link. Notes The Ethereum Yellow Paper Link. Notes	
21/11	Machine Learning Security and Wrap up | Slides	SoK: Security and Privacy in Machine Learning. Link. Adversarial Examples Are Not Bugs, They Are Features. Link. Stealing Machine Learning Models via Prediction APIs. Link. Notes	
28/11	Project Presentation		
Final Exam		TBA	

Grading

In-class quizzes	8%
assignments (~3)	12%
Midterm exam	20%
Final exam	35%
Group Project	25%

Policies

Late Policy: All homework assignments and project deliveries are assessed a 20% per-day late penalty, up to a maximum of 3 days. Students with legit reasons who contact the instructor before the deadline may apply for an extension.

Academic Integrity Policy Students are required to follow the university guidelines on academic conduct at all times. Students failing to meet these standards will automatically receive a 'F' grade for the course.

Note that students are explicitly forbidden to copy anything from the Internet (e.g., source code) for the purposes of completing an assignment. Students can discuss methodologies with classmates, but each student must do the work independently. The student will receive the same penalty if he/she let others copy the assignment.

Ethics Statement This course considers topics involving security and privacy. Along the semester we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.

When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from the instructor.
