Subject Description Form

Subject Code	COMP3334
Subject Title	Computer Systems Security
Credit Value	3
Level	3
Pre-requisite / Co-requisite / Exclusion	**Pre-requisite**: Basic understanding of modern operating systems is preferred
Objectives	To equip students with a foundational understanding of the threats to computer systems. Students will be equipped to: 1. understand the practical principles and models for protecting computer systems from various forms of attacks; 2. understand the major security issues and problems in computer systems, and the countermeasures to mitigate the corresponding attacks; and 3. acquire practical skills in using various tools and resources to analyse the security of computer systems, particularly the web systems.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/academic knowledge and skills* (a) understand the major security threats to computer systems and software, and the countermeasures to mitigate the corresponding attacks; (b) understand the major security threats to web systems and the countermeasures to mitigate the corresponding attacks; (c) understand and apply basic cryptographic techniques to secure information of computer systems; *Attributes for all-roundedness* (d) combine various security mechanisms to address the security requirements of computer systems; and (e) realise potential threats of new systems and the state-of-the-art technologies for protecting computer systems.
Subject Synopsis/ Indicative Syllabus	**Topic** **1. Overview** Security goals and policies, types of attacks, threat models. **2. Cryptography** Classical cryptography, modern symmetric cryptography, public-key cryptography, and steganography.

	3. Authentication Password systems, one-time passwords, strong password protocols, and password authentication protocols, key agreement protocols. **4. Software exploits and countermeasures** Buffer overflow, memory protection and corruption, principles of secure coding, code audit and review, malicious codes, rootkits, malwares, and browser security. **5. Web security** Input validation, SQL injection, cross-site scripting, cross-site request forgery, unvalidated redirects and forwards. **6. Case study & Advanced topics** Blockchain, Merkle tree, blind signatures, ring signatures, and zero knowledge proof, etc. Workshops: A series of workshops will be given to let students acquire practical experience on the different topics.
Teaching/ Learning Methodology	The course will emphasise on both the principles and practices of computer system security. The principles will be covered mainly through the lectures and problem-solving activities in the tutorials, whereas the practice aspects will be taught through a series of workshops which are designed to reinforce what has been taught in the lectures and to help students acquire practical skills and group projects.
Assessment Methods in Alignment with Intended Learning Outcomes	See table below.

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed				
		a	b	c	d	e
Continuous Assessment	**60%**					
1. Assignments	25%	✓	✓	✓		✓
2. Workshops	10%				✓	
3. Project	25%				✓	✓
Examination	**40%**	✓	✓	✓		✓
Total	100%					

The examination and assignments are designed to evaluate the students' understanding on the principles undergirding the web and software security. The workshops, on the other hand, are designed to evaluate the students' practical skills on solving computer system security problems.

Student Study Effort Expected	Class contact:	
	▪ Lectures	39 Hrs.
	▪ Tutorials/Workshops	0 Hrs.

	Other student study effort:	
	▪ Self-study (average 6 hours per week)	66 Hrs.
	Total student study effort	105 Hrs.
Reading List and References	**Textbooks:** 1. Bishop, Matt, *Introduction to Computer Security*, Addison Wesley, 2005. **Reference Books:** 1. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson 2017. 2. W. Du, Computer & Internet Security: A Hands-on Approach, 2nd ed., Wenliang Du 2019. 3. D. A. Tevault, Mastering Linux Security and Hardening: Protect your Linux systems from intruders, malware attacks, and other cyber threats, 2nd ed., Packt Publishing 2020. 4. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley 2020. 5. G. Hoglund and G. McGraw, *Exploiting Software*, Addison Wesley, 2004.	