Subject Description Form

Subject Code	COMP3334
Subject Title	Computer Systems Security
Credit Value	3
Level	3
Pre-requisite	Basic understanding of modern operating systems
Co-requisite/ Exclusion	Nil
Objectives	To equip students with a foundational understanding of the threats to computer systems. Students will be equipped to: • Understand the practical principles and models for protecting computer systems from various forms of attacks • Understand the major security issues and problems in computer systems, and the countermeasures to mitigate the corresponding attacks • Acquire practical skills in using various tools and resources to analyze the security of computer systems, particularly the web systems
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand the major security threats to computer systems and software, and the countermeasures to mitigate the corresponding attacks 2. Understand the major security threats to web systems and the countermeasures to mitigate the corresponding attacks 3. Acquire practical skills, such as reverse engineering of software, forensics of computer systems, malware analysis, security of web servers, and security of web browsers Category B: Attributes for all-roundedness 4. Acquire critical and independent analytical skills in the process of analyzing the security problems in computer systems 5. Acquire the skill of synthesizing various security problems into a small set of fundamental security issues and solutions

Subject Synopsis/ Indicative Syllabus

Syllabus:

Topic
1. Overview Security goals and policies, types of attacks, threat models, and review of basic cryptography
2. Authentication Password systems, one-time passwords, strong password protocols, and password authentication protocols
3. Access control and authorization Access control list, role/attribute/capability-based access control, and multi-layer privileged model.
4. Software exploits and countermeasures Buffer overflow, memory protection and corruption, principles of secure coding, code audit and review, software penetration testing, 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, broken authentication and session management, and security misconfiguration.

Workshops:
A series of workshops will be given to let students acquire practical experience on the different topics.

Teaching/ Learning Methodology

The course will emphasize 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

Specific Assessment Methods/Tasks	**% Weighting**	**Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)**				
		1	**2**	**3**	**4**	**5**
1. Continuous Assessment						
• Assignments	25%	✓	✓	✓		✓
• Workshops	10%				✓	
• Project	25%				✓	✓
2. 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 Hours
	Other student study effort:	
	• Self-study (average 6 hours per week)	94 Hours
	Total student study effort:	**133 Hours**
Reading List and References	**Textbooks:** 1. M. Bishop, *Introduction to Computer Security*, Addison Wesley 2005. **Reference Books:** 1. R. Anderson, *Security Engineering*, Second Edition, Wiley 2008. 2. C. Kaufman, R. Perlman and M. Speciner, *Network Security: Private Communication in a Public World,* Second Edition, Prentice Hall PTR 2003. 3. G. Hoglund and G. McGraw, *Exploiting Software*, Addison Wesley 2004. 4. G. McGraw, *Software Security*, Addison Wesley 2006. 5. S. Mann and E. Mitchell, *Linux System Security*, Prentice Hall PTR 2000. 6. B. Schneier*, Applied Cryptography*, Second Edition, Wiley 1996. 7. B. Schneier, *Secrets and Lies*, Wiley 2000. 8. D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook*, Wiley 2008.	
Last Updated	July 2016	
Prepared by	COMP Department	