MULTIMEDIA UNIVERSITY®

COURSE INFORMATION

1 .	**Name of Course**	Computer Security
2 .	**Course Code**	TSN3251
3 .	**Type of Course** **(e.g. : Core, major, elective etc.)**	Specialization Elective – B.CS Information Systems
4 .	**Synopsis**	This course provides a broad exposure to security from a computing perspective. Upon completion of the course, the students will be able to understand security concepts and explain them.
5 .	**Version** **(State the date of theSenate's approval - previous and the current approval date)**	Current: January 2018 Previous: June 2016
6 .	**Name(s) of Academic Staff**	Ian Tan Kim Teck, Kannan Ramakrishnan
7 .	**Semester and Year Offered**	Trimester 1, (Delta Year)
8 .	**Credit Value**	4
9 .	**Pre-Requisite**	TCP1101 Programming Fundamentals
10 .	**Objective of the course in the programme:**	
	i. To understand the building blocks and mathematical foundation of cryptography. ii. To understand the fundamental concepts of Computer Security covering Application Software, System Software, Network and Database Security. iii. To identify the different security threats and issues related to Computer Security and their countermeasures.	
11 .	**Justification for including the course in the programme:**	
	To provide students with more in-depth theoretical foundations on computer security.	

12 .	**Course Learning Outcomes (CLO)**	**Domain**	**Level**
	CLO1: Explain the building blocks of cryptography and the use of encryption standards.	Cognitive	2
	CLO2: Describe and interpret fundamental concepts related to computer, networking and database security.	Cognitive	3
	CLO3: Identify the potential threats and security issues in networks and databases and apply countermeasures to the threats.	Cognitive	3

13 . **Mapping of the Course Learning Outcomes to the Programme Learning Outcomes, Teaching Methods and Assessment:**

Course Learning Outcomes (CLO) (Must tally with CLOs in item 12)	Programme Learning Outcomes (PLO)												Teaching Methods	Assessment Method
	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10	PLO11	PLO12		
CLO1							✓						Lecture, Tutorial, Practical	Quiz, Test, Assignment and Final Exams
CLO2							✓						Lecture, Tutorial	Quiz, Test and Final Exams
CLO3								✓	✓				Lecture, Tutorial, Practical	Quiz and Final Exams
CLO4														
Total							**2**	**1**	**1**				*Indicate the relevancy between the CLO and PLO by ticking "✓" the appropriate relevant box (This description must be read together with standards 2.1.2, 2.2.1, and 2.2.2 in Area 2 – pages 16 & 18 of COPPA 2.0)*	

14 . **Transferable Skills:**

Good grasp of security jargon, appreciation of the need to focus on security, able to present security issues.

15 . **Distribution of Student Learning Time (SLT)**

	Course Content Outline	**CLO	Teaching and Learning Activities – Guided Learning (F2F)*				Guided Learning (NF2F)*	Independent Learning (NF2F)*	Total SLT
			*L	*T	*P	*O			
1	**Overview** Introduction to computer security. Concept of confidentiality, integrity and availability. Discussion on vulnerabilities, threats, controls.	**CLO2**	2		1		6	3	12
2	**Elementary Cryptography** Terminology and background. Stream and block ciphers. Mono-alphabetic substitution and cryptanalysis methods. Polyalphabetic substitution and cryptanalysis methods. Transposition ciphers and cryptanalysis methods	**CLO1**	4		4			8	16
3	**Symmetric Cryptography** Classical to modern ciphers (product ciphers). DES as a case study of modern ciphers. Evolution of modern ciphers, Triple DES and AES	**CLO1**	2	2				4	8

4	**Asymmetric Cryptography** Mathematical foundation in finite field arithmetic, prime numbers and primality tests. Introduction to Public-Key cryptography and usage. RSA as a case study of asymmetric ciphers, timing attacks on RSA and countermeasures against timing attacks.	**CLO1**	6	2				8	16
5	**Program Security** Securing programs, non-malicious software errors, malicious software (Virus, Trojans, etc.) and controls against program threats.	**CLO2, CLO3**	2		3		2	5	12
6	**Database Security** Introduction to databases security requirements. Inference attacks and countermeasures to inference attacks. Database SQL Injection Attacks	**CLO2, CLO3**	2	2				4	8
7	**Operating System Security** Memory protection and file access protection. Authentication: passwords, biometrics and multi-modal authentication	**CLO2, CLO3**	4		2		4	6	16
8	**Network Security** Issues: reconnaissance, threats in transit, impersonation, message confidentiality threats, message integrity threats, denial of service. Controls: encryption, firewalls, intrusion detection systems	**CLO2, CLO3**	4		4			8	16
9	**Security Administration** Security planning, risk analysis & economies of security, security policies & physical security.	**CLO2, CLO3**	2	2				4	8
								Total SLT	**112**

SUMMATIVE ASSESSMENT

1. Continuous Assessment	**Percentage %**	**Total SLT**
Quizzes	15%	4
Assignments	15%	12
Test	20%	8
	Total SLT for Continuous Assessment	**24**

2. Final Assessment	**Percentage %**	**Total SLT**	
		F2F	**ILT**
Final Exam	50%	2	22
	Total SLT for Final Assessment (F2F + NF2F)	**24**	

	Grand Total	**100%**	**160**
	****Indicate the CLO based on the CLO's numbering in Item 12.** ***L= Lecture, *T= Tutorial, *P= Practical, *O= Others, F2F*= Face to Face, NF2F*= Non Face to Face**		
16 .	**Identify Special Requirement to Deliver the Course (e.g., software, nursery, computer lab, simulation room):** VirtualBox, Ubuntu, Wireshark		
17 .	**Main References:** William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Prentice Hall; 2nd edition (November 19, 2011), ISBN-10: 0132775069.		
18 .	**Additional References:**		
	William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall; 6th edition (March 16, 2013), ISBN-10: 0133354695. Charles P. Pfleeger and Shari Lawrence Pfleeger. Security in Computing, Prentice Hall; 4th edition (October 23, 2006), ISBN-10: 0132390779.		

Note:

	Cells shaded light grey contain formulas / fixed values. Edit these formulas only if needed.