Subject Description Form

Subject Code	COMP4334
Subject Title	Principles and Practice of Internet Security
Credit Value	3
Level	4
Pre-requisite / Co-requisite/ Exclusion	Pre-requisite: COMP3334 Co-requisite/Exclusion: Nil
Objectives	To equip students with a foundational understanding of the threats to the Internet infrastructure. Students will be equipped to: • understand the practical principles, models, cryptographic methods for protecting Internet from various forms of attacks; • understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; and • acquire practical skills in using various tools and resources to analyze the security of Internet protocols.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/academic knowledge and skills* (a) acquire a foundational understanding of the three cryptographic primitives: secret-key encryption, public-key encryption, and one-way hash functions; (b) understand the major security issues in implementing the four major security functions: secrecy, identity authentication, message authentication, and nonrepudiation; (c) understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; (d) acquire practical skills, such as setting up a secure private network using firewalls, secure tunnels, and end-to-end secure applications, implementing and/or integrating security functions, and assessment of system security; and (e) understand the major threats to the Internet-wide security today, such as denial-of-service attacks and DNS insecurity. *Attributes for all-roundedness* (f) acquire critical and independent analytical skills in the process of analyzing the security problems in the Internet;

(g) acquire the skill of synthesizing various security problems into a small set of fundamental security issues and solutions.

Subject Synopsis/ Indicative Syllabus

Topic
1. Overview Types of attacks; threat models; the role of cryptography in network security.
2. Cryptographic functions and services Symmetric encryption, block cipher; hash functions; message authentication codes; public-key encryption, digital signatures, and authentication protocols.
3. IP and link-layer security IP security and Internet key exchange protocols; routing security; wireless network security.
4. End-to-end security TCP security; Secure Socket Layer; examples of secure application protocols; e.g., Secure Shell, Kerberos, and Pretty Good Privacy.
5. Other topics DNS security, denial-of-service attacks, botnet, firewalls and intrusion detection/prevention systems.

Workshops:

A series of workshops on Web security will be given to let students acquire practical experience.

Teaching/ Learning Methodology

The course will emphasize on both the principles and practices of network and 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 on Web security 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)						
		a	b	c	d	e	f	g
1. Assignments	25%	✓	✓	✓		✓	✓	✓
2. Workshops	10%				✓			
3. Project	25%				✓	✓	✓	✓
4. Examination	40%	✓	✓	✓		✓	✓	✓
Total	100 %							

	The examination and assignments are designed to evaluate the students' understanding on the principles undergirding the network and system security. The workshops on Web security and group projects, on the other hand, are designed to evaluate the students' practical skills on solving Internet security problems.	
Student Study Effort Expected	Class contact:	
	▪ Lectures	39 Hrs.
	▪ Tutorials/Workshops	0 Hrs.
	Other student study effort:	
	▪ Self-study (around 7 hours per week)	94 Hrs.
	Total student study effort	133 Hrs.
	Textbooks: 1. N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley 2010.	
Reading List and References	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. D. B. Chapman and E. D. Zwicky, Building Internet Firewalls. Second Edition, O'Reilly & Associates 2000. 4. W. Cheswick and S. Bellovin, Firewalls and Internet Security, Second Edition, Addison Wesley 2003. 5. B. Schneier, Applied Cryptography, Second Edition, Wiley 1996. 6. B. Schneier, Secrets and Lies, Wiley 2000. 7. Young and M. Yung, Malicious Cryptography, Wiley 2004. 8. D. Stinson, Cryptography: Theory and Practice, Third Edition, Chapman and Hall/CRC 2006. 9. B. Forouzan, Cryptography and Network Security, McGraw-Hill 2008. 10. C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment, Springer 2003.	