Subject Description Form

Subject Code	COMP444
Subject Title	Internet Infrastructure Security
Credit Value	3
Level	4
Pre-requisite / Co-requisite/ Exclusion	Pre-requisite: COMP312 Co-requisite/Exclusion: Nil
Objectives	To equip students with a foundational understanding of the threats to the Internet infrastructure security and the countermeasures. Students will be equipped to: • understand and evaluate the current Internet infrastructure from the network security point of view; • acquire practical experience in implementing, setting up, and testing network security measures.
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; (e) understand the major threats to the Internet-wide security today, such as denial-of-service attacks and Internet worms. *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. Preliminaries Types of attacks; threat models; the role of cryptography in network security.
2. Cryptographic functions and services Block cipher; block cipher modes; hash functions; message authentication codes; a secure channel and the implementation issues.
3. Key negotiation and management Diffie-Hellman algorithm; RSA algorithm; key negotiation protocols; key management issues; Public Key Infrastructure.
4. IP and lower-layer security IP security and Internet key exchange protocols; routing security; wireless network security; quantum cryptography.
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. Advanced topics Internet worms; denial-of-service; DDOS.

Teaching/ Learning Methodology

The course will emphasize on both the principles and practices of internet security.

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	60%	✓	✓	✓		✓	✓	✓
2. Exercises					✓			
3. Project					✓	✓	✓	✓
4. Mid-term								
4. Examination	40%	✓	✓	✓		✓	✓	✓
Total	100 %							

Student Study Effort Expected

Class contact:	
▪ Lectures	39 Hrs.
▪ Tutorials/Workshops	0 Hrs.
Other student study effort:	

	▪ Self-study	66 Hrs.
	Total student study effort	105 Hrs.
Reading List and References	1. N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley 2010. 2. R. Anderson, Security Engineering, Second Edition, Wiley 2008. 3. M. Bishop, Introduction to Computer Security, Addison Wesley 2005. 4. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a Public World, Second Edition, Prentice Hall PTR 2003. 5. D. B. Chapman and E. D. Zwicky, Building Internet Firewalls. Second Edition, O'Reilly & Associates 2000. 6. W. Cheswick and S. Bellovin, Firewalls and Internet Security, Second Edition, Addison Wesley 2003. 7. B. Schneier, Applied Cryptography, Second Edition, Wiley 1996. 8. B. Schneier, Secrets and Lies, Wiley 2000. 9. A. Young and M. Yung, Malicious Cryptography, Wiley 2004. 10. D. Stinson, Cryptography: Theory and Practice, Third Edition, Chapman and Hall/CRC 2006. 11. B. Forouzan, Cryptography and Network Security, McGraw-Hill 2008. 12. C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment, Springer 2003.	