Subject Description Form

Subject Code	COMP5355
Subject Title	Cyber and Internet Security
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil (but some knowledge in programming, computer networking, or operating systems is preferable)
Objectives	To equip students with a fundamental understanding of Cyber and Internet security and practical skills of handling Cyber and Internet security issues. Students will be equipped to: • describe the concepts and principles of Cyber and Internet security; • explain the attack surface at different network layers; • understand the security mechanisms in major TCP/IP protocols; • develop practical skills to analyze network traffic for dissecting the attacks exploiting TCP/IP protocols and designing defense mechanisms; • understand the major threats to web applications; • analyze the attacks targeting on web applications and design defense mechanisms; • develop practical skills to conduct penetration testing and set up network firewall/IDS/IPS; • understand the major threats to systems (e.g., PC, smartphone, etc.)
Intended Learning Outcomes	Upon completion of the subject, students will be able to: <u>Professional/academic knowledge and skills</u> a. Understand and apply fundamental cyber security concepts as well as advanced and specialized cyber security knowledge for formulating models and solutions. b. Analyse and solve cyber security problems through critical thinking, analytical thinking and creative thinking. c. Design and evaluate systems/applications to satisfy user needs and various requirements (e.g., detect attack, discover vulnerability, set up defense mechanisms, etc.). <u>Attributes for all-roundedness</u> d. Understand professional ethics, responsibilities and practice as well as legal and social issues. e. Engage in life-long independent learning for professional development.

<table>
<tr><td>Subject Synopsis/ Indicative Syllabus</td><td>1. Principle of Cyber Security and Privacy.

2. Attack surface at different network layers, including MAC, IP, TCP, Application layers.

3. Security mechanisms in TCP/IP protocols, including IP Security, Internet Key Exchange, routing security, SSL/TLS, and TCP security

4. Traffic analysis for analyzing the attacks.

5. Web security and major threats to web applications.

6. Network intrusion detection and prevention, firewalls, penetration testing.

7. Threats to systems (e.g., PC, smartphone, etc.)

8. Professionalism and legal/social issues (e.g., security certification)</td></tr>
<tr><td>Teaching/Learning Methodology</td><td>The course will be delivered as a combination of lectures, tutorials, labs, workshops, and class project. The course will emphasize on both the principles and practices of Cyber and Internet Security. The principles will be covered mainly through the lectures and the tutorials, whereas the practice aspects will be taught through labs and workshops. The class project will help students reinforce what they have learnt, including both principles and practical skills.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="5">Intended subject learning outcomes to be assessed (Please tick as appropriate)</td></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td></tr>
<tr><td>1. Assignments</td><td>30</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>2. Class project</td><td>25</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>3. Examination</td><td>45</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>Total</td><td>100</td><td colspan="5"></td></tr>
</table>

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

The assessment is based on the following:

1. Continuous assessment by assignments and class projects;

2. Final examination</td></tr>
<tr><td rowspan="3">Student Study Effort Expected</td><td>Class contact:</td><td></td></tr>
<tr><td>▪ Lecture</td><td>26 Hrs.</td></tr>
<tr><td>▪ Tutorial/Lab/Workshop</td><td>13 Hrs.</td></tr>
</table>

	Other student study effort:	
	▪ Assignment	25 Hrs.
	▪ Class project	40 Hrs.
	Total student study effort	**104 Hrs.**
Reading List and References	1. Wenliang Du, Computer Security: A Hands-on Approach, CreateSpace Independent Publishing Platform, 2017 2. William Stallings, Cryptography and Network Security: Principles and Practice, 5th edition, Prentice Hall, 2010. 3. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2008 4. Dieter Gollmann, Computer Security, Wiley, 2011 5. Proceedings of IEEE Symposium on Security and Privacy 6. Proceedings of USENIX Security Symposium 7. Proceedings of ISOC Network and Distributed System Security Symposium 8. Proceedings of ACM Conference on Computer and Communications Security 9. Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks 10. Proceedings of Annual Computer Security Applications Conference 11. Proceedings of European Symposium on Research in Computer Security 12. Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses	