Subject Description Form

Subject Code	COMP 5353
Subject Title	Internet Security: Principles and Practice
Credit Value	3
Level	5
Pre-requisite/ Exclusion	Prerequisite: COMP5311 Internet Infrastructure and Protocols Exclusion: COMP5351 Internet Infrastructure Security
Objectives	The overall objective of this course is to equip students with foundational principles and practical skills on security issues relevant to the current Internet infrastructure, such as 1. The three main cryptographic functions: secret key, public key, and hash; 2. The four main network security services: secrecy, message integrity, authentication, and nonrepudiation; and 3. Public key infrastructure, IP network security, SSL/TLS, web server and browser security, system security, and network intrusion and defense.
Intended Learning Outcomes	Upon successful completion of this course, students should be able to: a) Read and understand articles in professional computer and network security magazines, such as IEEE Security & Privacy and SC Magazine. b) Use Wireshark to analyze network attacks; build, design, and test the security of web applications and web services; and perform basic site penetration tests. c) Take on a self-study on more advanced network security topics that require foundational understanding of cryptographic algorithms and security of network protocols.
Subject Synopsis/ Indicative Syllabus	• Cryptographic preliminaries: threat analysis, security goals, security verses privacy, basic cryptographic functions, public key infrastructure, and digital signatures • IP network and end-to-end security: IP Security, Internet Key Exchange, routing security, SSL/TLS, and TCP security • Web and system security: Windows and Linux systems security, web server security, and OWASP top 10 vulnerability for web services • Network intrusions: Intrusion detection and prevention, site penetration tests, firewalls, stateful inspection
Teaching/Learning Methodology	Class activities, including lectures, tutorials, workshops, and guest seminars

<table>
<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="3">Intended subject learning outcomes to be assessed</td></tr>
<tr><td>a</td><td>b</td><td>c</td></tr>
<tr><td>Assignments, Tests & Projects</td><td>55</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Final Examination</td><td>45</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Total</td><td>100</td><td colspan="3"></td></tr>
</table>
</td></tr>
<tr><td rowspan="5">Student study effort expected</td><td colspan="2">Class Contact:</td></tr>
<tr><td>Class activities (lecture, tutorial, lab)</td><td>39 hours</td></tr>
<tr><td colspan="2">Other student study effort:</td></tr>
<tr><td>Assignments, Quizzes, Projects, Exams</td><td>65 hours</td></tr>
<tr><td>Total student study effort</td><td>104 hours</td></tr>
<tr><td>Reading list and references</td><td colspan="2">(1) R. Anderson. Security Engineering, Second Edition, Wiley, 2008.
(2) M. Bishop. Introduction to Computer Security, Addison Wesley, 2005.
(3) B. Chapman and E. Zwicky. Building Internet Firewalls. Second Edition, O’Reilly & Associates, 2000.
(4) N. Ferguson, B. Schneier, and T. Kohno. Cryptography Engineering, Wiley, 2010.
(5) C. Kaufman, R. Perlman, and M. Speciner. Network Security: Private Communication in a Public World, Second Edition, Prentice Hall PTR, 2002.

Supplementary articles from IEEE/ACM publications</td></tr>
</table>