

## Subject Description Form

<b>Subject Code</b>	COMP4334		
<b>Subject Title</b>	Principles and Practice of Internet Security		
<b>Credit Value</b>	3		
<b>Level</b>	4		
<b>Pre-requisite / Co-requisite / Exclusion</b>	<b>Pre-requisite:</b> COMP3334		
<b>Objectives</b>	<p>To equip students with a foundational understanding of the threats to the Internet infrastructure. Students will be equipped to:</p> <ol style="list-style-type: none"> <li>1. understand the practical principles, models, cryptographic methods for protecting Internet from various forms of attacks;</li> <li>2. 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</li> <li>3. acquire practical skills in using various tools and resources to analyse the security of Internet protocols.</li> </ol>		
<b>Intended Learning Outcomes</b>	<p>Upon completion of the subject, students will be able to:</p> <p><i>Professional/academic knowledge and skills</i></p> <ol style="list-style-type: none"> <li>(a) acquire a foundational understanding of the cryptographic primitives, security functions and Internet threats;</li> <li>(b) 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;</li> <li>(c) 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;</li> </ol> <p><i>Attributes for all-roundedness</i></p> <ol style="list-style-type: none"> <li>(d) acquire critical and independent analytical skills in the process of analysing the security problems in the Internet; and</li> <li>(e) synthesise various security problems into a small set of fundamental security issues and propose feasible security mechanisms and solutions.</li> </ol>		
<b>Subject Synopsis/ Indicative Syllabus</b>	<table border="1" style="width: 100%;"> <tr> <td style="text-align: center;"><b>Topic</b></td> </tr> <tr> <td>1. <b>Overview</b> Types of attacks; threat models; the role of cryptography in network security.</td> </tr> </table>	<b>Topic</b>	1. <b>Overview</b> Types of attacks; threat models; the role of cryptography in network security.
<b>Topic</b>			
1. <b>Overview</b> Types of attacks; threat models; the role of cryptography in network security.			

	<p><b>2. Cryptographic Functions and Services</b></p> <p>Symmetric encryption, block cipher; hash functions; message authentication codes; public-key encryption, digital signatures, and authentication protocols.</p> <p><b>3. IP and Link-Layer Security</b></p> <p>IP security and Internet key exchange protocols; routing security; wireless network security.</p> <p><b>4. End-to-End Security</b></p> <p>TCP security; Secure Socket Layer; examples of secure application protocols; e.g., Secure Shell, Kerberos, and Pretty Good Privacy.</p> <p><b>5. Other Topics</b></p> <p>DNS security, denial-of-service attacks, botnet, firewalls and intrusion detection/prevention systems.</p> <p>Workshops:</p> <p>A series of workshops on Web security will be given to let students acquire practical experience.</p>																																																						
<p><b>Teaching/ Learning Methodology</b></p>	<p>The course will emphasise 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.</p>																																																						
<p><b>Assessment Methods in Alignment with Intended Learning Outcomes</b></p>	<table border="1"> <thead> <tr> <th rowspan="2">Specific assessment methods/tasks</th> <th rowspan="2">% weighting</th> <th colspan="5">Intended subject learning outcomes to be assessed</th> </tr> <tr> <th>a</th> <th>b</th> <th>c</th> <th>d</th> <th>e</th> </tr> </thead> <tbody> <tr> <td><b>Continuous Assessment</b></td> <td><b>60%</b></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>1. Assignments</td> <td>25%</td> <td>✓</td> <td>✓</td> <td></td> <td>✓</td> <td>✓</td> </tr> <tr> <td>2. Workshops</td> <td>10%</td> <td></td> <td></td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>3. Project</td> <td>25%</td> <td></td> <td></td> <td>✓</td> <td>✓</td> <td>✓</td> </tr> <tr> <td><b>Examination</b></td> <td><b>40%</b></td> <td>✓</td> <td>✓</td> <td></td> <td>✓</td> <td>✓</td> </tr> <tr> <td>Total</td> <td>100%</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>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.</p>	Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed					a	b	c	d	e	<b>Continuous Assessment</b>	<b>60%</b>						1. Assignments	25%	✓	✓		✓	✓	2. Workshops	10%			✓			3. Project	25%			✓	✓	✓	<b>Examination</b>	<b>40%</b>	✓	✓		✓	✓	Total	100%					
Specific assessment methods/tasks	% weighting			Intended subject learning outcomes to be assessed																																																			
		a	b	c	d	e																																																	
<b>Continuous Assessment</b>	<b>60%</b>																																																						
1. Assignments	25%	✓	✓		✓	✓																																																	
2. Workshops	10%			✓																																																			
3. Project	25%			✓	✓	✓																																																	
<b>Examination</b>	<b>40%</b>	✓	✓		✓	✓																																																	
Total	100%																																																						

<b>Student Study Effort Expected</b>	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.
<b>Reading List and References</b>	<b>Textbooks:</b>	
	1. Stallings, William, <i>Cryptography and Network Security: Principles and Practice</i> , 6 <sup>th</sup> Edition, Pearson, 2013.	
	<b>Reference Books:</b>	
	1. Anderson, Ross J., <i>Security Engineering</i> , 2 <sup>nd</sup> Edition, Wiley, 2008.	
	2. Kaufman, Charlie, Perlman, Radia and Speciner, Mike, <i>Network Security: Private Communication in a Public World</i> , 2 <sup>nd</sup> Edition, Prentice Hall PTR 2003.	
	3. Zwicky, Elizabeth D., Cooper, Simon and Chapman, D. Brent, <i>Building Internet Firewalls</i> , 2 <sup>nd</sup> Edition, O'Reilly & Associates, 2000.	
	4. Cheswick, William and Bellovin, Steven M., <i>Firewalls and Internet Security</i> , 2 <sup>nd</sup> Edition, Addison Wesley, 2003.	
	5. Schneier, Bruce, <i>Applied Cryptography</i> , 2 <sup>nd</sup> Edition, Wiley, 1996.	
	6. Schneier, Bruce, <i>Secrets and Lies</i> , Wiley, 2000.	
	7. Young, Adam and Yung, Moti, <i>Malicious Cryptography</i> , Wiley, 2004.	
	8. Stinson, Douglas R., <i>Cryptography: Theory and Practice</i> , 3 <sup>rd</sup> Edition, Chapman and Hall/CRC, 2006.	
	9. Forouzan, Behrouz A., <i>Cryptography and Network Security</i> , McGraw-Hill, 2008.	
	10. Boyd, Colin and Mathuria, Anish, <i>Protocols for Authentication and Key Establishment</i> , Springer, 2003.	
11. Katz, Jonathan, and Yehuda Lindell. <i>Introduction to modern cryptography</i> . CRC press, 2nd Edition, 2020.		