

The Hong Kong Polytechnic University

Subject Description Form

Please read the notes at the end of the table carefully before completing the form.

Subject Code	COMP6712
Subject Title	Advanced Security and Privacy
Credit Value	3
Level	6
Pre-requisite/ Co-requisite/ Exclusion	Knowledge in COMP2432 (Operating Systems), COMP2322 (Computer Networking) and COMP3211 (Software Engineering) or equivalent.
Objectives	<ol style="list-style-type: none"> 1. To motivate students to understand the principles, methodologies and techniques of security and privacy. 2. To apply the acquired knowledge and skills to discover and solve security and privacy problems in various applications.
Intended Learning Outcomes <i>(Note 1)</i>	<p>Upon completion of the subject, students will be able to:</p> <p><u>Professional/academic knowledge and skills</u></p> <p>(a) Understand fundamental principles, methodologies, and techniques of security and privacy, and develop new insights into complex and abstract issues.</p> <p>(b) Produce creative and original solutions to real problems in the context of new circumstances, communicating appropriately to academic and non-academic audiences</p> <p>(c) Design and implement security and privacy techniques to deal with very complex practical problems and professional issues.</p> <p><u>Attributes for all-roundedness</u></p> <p>(d) Understand professional ethics, responsibilities, and practice as well as legal and social issues, and assume full accountability for their work.</p> <p>(e) Engage in life-long independent learning for professional development, and demonstrate leadership and originality in responding to new and unforeseen circumstances.</p>
Subject Synopsis/ Indicative Syllabus	<ol style="list-style-type: none"> 1. Introductory <p>Principles of security and privacy; Access control; Security policies; Basic cryptography; Authentication; Professionalism and legal/social issues</p>

<p>(Note 2)</p>	<p>2. Advanced Attack surfaces at different network layers; Traffic analysis for detecting and dissecting network attacks; Network defense mechanisms; Secure software architecture and design; Secure coding and testing,</p> <p>3. Applications Penetration testing; Vulnerability analysis; Malware detection; Latest attacks on various computing techniques and applications and the countermeasures (e.g., Blockchain Security and Privacy, AI Security and Privacy, etc.)</p>																																															
<p>Teaching/Learning Methodology</p> <p>(Note 3)</p>	<p>Lectures/Tutorials/Seminars/Laboratories/Project</p>																																															
<p>Assessment Methods in Alignment with Intended Learning Outcomes</p> <p>(Note 4)</p>	<table border="1" data-bbox="520 819 1474 1294"> <thead> <tr> <th rowspan="2">Specific assessment methods/tasks</th> <th rowspan="2">% weighting</th> <th colspan="6">Intended subject learning outcomes to be assessed (Please tick as appropriate)</th> </tr> <tr> <th>a</th> <th>b</th> <th>c</th> <th>d</th> <th>e</th> <th></th> </tr> </thead> <tbody> <tr> <td>1. Assignments</td> <td>20%</td> <td>✓</td> <td>✓</td> <td>✓</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>2. Class Projects</td> <td>45%</td> <td>✓</td> <td>✓</td> <td>✓</td> <td>✓</td> <td>✓</td> <td></td> </tr> <tr> <td>3. Final Exam</td> <td>35%</td> <td>✓</td> <td>✓</td> <td></td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Total</td> <td>100 %</td> <td colspan="6"></td> </tr> </tbody> </table> <p>Assignment(s): assessment of the studies with respect to the understanding of the relevant subject matters including the principles, methodologies, and techniques by proving answers to the assignment questions.</p> <p>Project: assessment of the ability of solving real problems by using learned techniques and developing practical solutions.</p> <p>Exam: assessment of the overall performance by exam.</p>		Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)						a	b	c	d	e		1. Assignments	20%	✓	✓	✓	✓			2. Class Projects	45%	✓	✓	✓	✓	✓		3. Final Exam	35%	✓	✓		✓			Total	100 %						
Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)																																														
		a	b	c	d	e																																										
1. Assignments	20%	✓	✓	✓	✓																																											
2. Class Projects	45%	✓	✓	✓	✓	✓																																										
3. Final Exam	35%	✓	✓		✓																																											
Total	100 %																																															
<p>Student Study Effort Expected</p>	<table border="1" data-bbox="520 1648 1474 2114"> <tr> <td colspan="2">Class contact:</td> <td></td> </tr> <tr> <td>▪ Lecture</td> <td></td> <td>26 Hrs.</td> </tr> <tr> <td>▪ Tutorial/Seminar/ Laboratory</td> <td></td> <td>13 Hrs.</td> </tr> <tr> <td colspan="2">Other student study effort:</td> <td></td> </tr> <tr> <td>▪ Reading</td> <td></td> <td>40 Hrs.</td> </tr> <tr> <td>▪ Preparing project, assignment, exam</td> <td></td> <td>43 Hrs.</td> </tr> <tr> <td colspan="2">Total student study effort</td> <td>122 Hrs.</td> </tr> </table>		Class contact:			▪ Lecture		26 Hrs.	▪ Tutorial/Seminar/ Laboratory		13 Hrs.	Other student study effort:			▪ Reading		40 Hrs.	▪ Preparing project, assignment, exam		43 Hrs.	Total student study effort		122 Hrs.																									
Class contact:																																																
▪ Lecture		26 Hrs.																																														
▪ Tutorial/Seminar/ Laboratory		13 Hrs.																																														
Other student study effort:																																																
▪ Reading		40 Hrs.																																														
▪ Preparing project, assignment, exam		43 Hrs.																																														
Total student study effort		122 Hrs.																																														

<p>Reading List and References</p>	<ol style="list-style-type: none"> 1. Wenliang Du, Computer Security: A Hands-on Approach, CreateSpace Independent Publishing Platform, 2017 2. Matt Bishop, Computer Security: Art and Science, Addison-Wesley; 2nd edition, 2018. 4. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 3rd edition, 2020 5. William Stallings, Cryptography and Network Security: Principles and Practice, 5th edition, Prentice Hall, 2010. 6. Dieter Gollmann, Computer Security, Wiley, 2011 7. 6. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002. 8. Proceedings of IEEE Symposium on Security and Privacy 9. Proceedings of USENIX Security Symposium 10. Proceedings of ISOC Network and Distributed System Security Symposium 11. Proceedings of ACM Conference on Computer and Communications Security 12. Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks 13. Proceedings of Annual Computer Security Applications Conference 14. Proceedings of European Symposium on Research in Computer Security 15. Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses
---	--

Note 1: Intended Learning Outcomes

Intended learning outcomes should state what students should be able to do or attain upon subject completion. Subject outcomes are expected to contribute to the attainment of the overall programme outcomes.

Note 2: Subject Synopsis/Indicative Syllabus

The syllabus should adequately address the intended learning outcomes. At the same time, overcrowding of the syllabus should be avoided.

Note 3: Teaching/Learning Methodology

This section should include a brief description of the teaching and learning methods to be employed to facilitate learning, and a justification of how the methods are aligned with the intended learning outcomes of the subject.

Note 4: Assessment Method

This section should include the assessment method(s) to be used and its relative weighting, and indicate which of the subject intended learning outcomes that each method is intended to assess. It should also provide a brief explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes.