

## Subject Description Form

<b>Subject Code</b>	COMP4332
<b>Subject Title</b>	Mobile Security: Principles and Practice
<b>Credit Value</b>	3
<b>Level</b>	4
<b>Pre-requisite / Co-requisite / Exclusion</b>	<b>Pre-requisite:</b> COMP1011 and COMP2322 and COMP2432/COMP1411 and COMP3334
<b>Objectives</b>	<p>To equip students with a foundational understanding of mobile security and practical skills of handling security issues in mobile communications. Students will be equipped to:</p> <ul style="list-style-type: none"> <li>• describe the concepts and principles of mobile security;</li> <li>• understand the security architecture and threat model of mobile networks;</li> <li>• explain the security models of popular mobile operating systems, applications, and services;</li> <li>• analyze the threats to popular mobile operating systems, applications, and services; and</li> <li>• develop practical skills to detect attacks, to assess the security risk of mobile applications and services, and to analyze mobile malware.</li> </ul>
<b>Intended Learning Outcomes</b>	<p>Upon completion of the subject, students will be able to:</p> <p><u>Professional/academic knowledge and skills</u></p> <ul style="list-style-type: none"> <li>(a) understand the security architectures of cellular networks and WiFi networks along with the major threats in mobile communication;</li> <li>(b) explain the security model of the Android system, iOS systems, and their applications;</li> <li>(c) analyze Android applications, evaluate the threats to them, and dissect malware; and</li> <li>(d) identify major security and privacy issues in popular mobile services and applications.</li> </ul> <p><u>Attributes for all-roundedness</u></p> <ul style="list-style-type: none"> <li>(e) acquire critical thinking and analytical skills, and improve technical writing as well as presentation skills.</li> </ul>

<b>Subject Synopsis/ Indicative Syllabus</b>	<b>Topic</b>	<b>Duration of Lectures</b>
	<b>1. Overview of Mobile Communication and its Security</b> Mobile communication concepts, Security goals, types of attacks, threat models, and review of basic cryptography.	2
	<b>2. Cellular Networks Security</b> Access control and authentication in cellular networks, 3G/4G networks and their security architectures, attacks on 3G/4G networks.	4
	<b>3. WiFi Network Security</b> 802.11 protocols, WEP, WPA/WPA2, WiFi network attacks and threat assessment.	
	<b>4. Android Security</b> Android system, Android security model, Android apps analysis, Android application reverse engineering and monitoring, Android apps threat assessment.	8
	<b>5. iOS Security</b> iOS system, iOS security model, iOS application analysis.	2
	<b>6. Mobile Malware</b> Taxonomy of mobile malware, mobile malware detection, static analysis of mobile malware, dynamic analysis of mobile malware.	4
	<b>7. Selected Topics on Mobile Security</b> Advanced or current topics on mobile security, such as Near field communication security, mobile device management and BYOD.	4
	<b>Total</b>	<b>26</b>
<b>Teaching/ Learning Methodology</b>	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 mobile 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.	

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
	<b>Continuous Assessment</b>	<b>100%</b>					
	1. Assignments	25%	✓	✓	✓	✓	✓
	2. Term Project	30%		✓	✓	✓	✓
	3. Examination	45%	✓	✓	✓	✓	✓
	4. Tutorial/Lab			✓	✓	✓	✓
	5. Workshops				✓	✓	✓
	<b>Total</b>	<b>100 %</b>					
<p>Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:</p> <p>Continuous assessments consist of assignments and a term project, which are designed to facilitate students to achieve intended learning outcomes. Despite not being assigned with an assessment weighting, lab exercise and workshop are designed to encourage students to acquire deep understanding of the relevant knowledge</p> <p>Examination will evaluate student's understanding and practical skills of security issues in mobile communications.</p>							
<b>Student Study Effort Expected</b>	Class contact:						
	▪ Lectures					26 Hrs.	
	▪ Tutorials/Lab/Workshops					13 Hrs.	
	Other student study effort:						
	▪ Assignment and Term Project					40 Hrs.	
	▪ Self-Study and Examination Preparation					39 Hrs.	
Total student study effort					118 Hrs.		
<b>Reading List and References</b>	<b>Reference Books:</b>						
	<ol style="list-style-type: none"> <li>1. Boudriga, Nouredine, <i>Security of Mobile Communications</i>, Auerbach Publications, 2010.</li> <li>2. Dubey, Abhishek and Misra, Anmol, <i>Android Security: Attacks and Defenses</i>, Auerbach Publications, 2013.</li> </ol>						

3. Dwivedi, Himanshu, Clark, Chris and Thiel, David, *Mobile Application Security*, McGraw-Hill Osborne Media, 2010.
4. Miller, Charlie, Blazakis, Dion, DaiZovi, Dino, Esser, Stefan, Iozzo, Vincenzo and Weinmann, Ralf-Philipp, *iOS Hacker's Handbook*, Wiley, 2012
5. Traynor, Patrick, McDaniel, Patrick and La Porta, Thomas, *Security for Telecommunications Networks*, Springer, 2008.
6. Kaufman, Charlie, Perlman, Radia and Speciner, Mike, *Network Security: Private Communication in a Public World*, Prentice Hall, 2002.
7. Forsberg, Dan, Horn, Günther, Moeller, Wolf-Dietrich and Niemi, Valtteri, *LTE Security*, Wiley, 2012.
8. Buttyán, Levente and Hubaux, Jean-Pierre, *Security and Cooperation in Wireless Networks*, Cambridge University Press, 2008.
9. Proceedings of *IEEE Symposium on Security and Privacy*
10. Proceedings of *USENIX Security Symposium*
11. Proceedings of *ISOC Network and Distributed System Security Symposium*
12. Proceedings of *ACM Conference on Computer and Communications Security*
13. Proceedings of *IEEE/IFIP International Conference on Dependable Systems and Networks*
14. Proceedings of *European Symposium on Research in Computer Security*
15. Proceedings of *International Symposium on Research in Attacks, Intrusions and Defenses*
16. Proceedings of *Annual Computer Security Applications Conference*
17. Chell, Dominic, Erasmus, Tyrone, Colley, Shaun and Whitehouse, Ollie, *The Mobile Application Hacker's Handbook*, 1<sup>st</sup> Edition, Wiley, 2015.