Subject Description Form

Subject Code	COMP4332
Subject Title	Mobile Security: Principles and Practice
Credit Value	3
Level	4
Pre-requisite / Co-requisite / Exclusion	**Pre-requisite**: COMP1011/COMP1012/ENG2002 & COMP2322 & COMP2432/COMP1411 & COMP3334
Objectives	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: 1. describe the concepts and principles of mobile security; 2. understand the security architecture and threat model of mobile networks; 3. explain the security models of popular mobile operating systems, applications, and services; 4. analyse the threats to popular mobile operating systems, applications, and services; and 5. develop practical skills to detect attacks, to assess the security risk of mobile applications and services, and to analyse mobile malware.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: <u>*Professional/academic knowledge and skills*</u> (a) understand the security architectures of cellular networks and WiFi networks along, and acquire practical skills to identify the major threats to mobile communication; (b) analyse the security models of the Android and iOS systems, and their applications; (c) analyse Android applications, evaluate the threats to them, and dissect malware; (d) identify major security and privacy issues in popular mobile services and applications; and <u>*Attributes for all-roundedness*</u> (e) acquire critical thinking and analytical skills, and improve technical writing as well as presentation skills.

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

Assessment Methods in Alignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed				
		a	b	c	d	e
Continuous Assessment	**100%**					
1. Assignments	25%	✓	✓	✓	✓	✓
2. Term Project	30%		✓	✓	✓	✓
3. Examination	45%	✓	✓	✓	✓	✓
4. Tutorial/Lab			✓	✓	✓	✓
5. Workshops				✓	✓	✓
Total	100 %					

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

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

Examination will evaluate student's understanding and practical skills of security issues in mobile communications.

Student Study Effort Expected

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.

Reading List and References

Reference Books:

1. Boudriga, Noureddine, *Security of Mobile Communications*, Auerbach Publications, 2010.

2. Dubey, Abhishek and Misra, Anmol, *Android Security: Attacks and Defenses*, Auerbach Publications, 2013.

	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*, 1st Edition, Wiley, 2015.