Subject Description Form

Subject Code	COMP4332
Subject Title	Mobile Security: Principles and Practice
Credit Value	3
Pre-requisite / Co-requisite/ Exclusion	Pre-requisite: COMP1011 Programming Fundamentals, and COMP2322 Computer Networking, and COMP2432 Operating Systems, and COMP3334 Computer Systems Security Co-requisite: Nil Exclusion: Nil
Objectives	To equip students with a fundamental understanding of mobile security and practical skills of handling security issues in mobile communications. Students will be equipped to: • describe the concepts and principles of mobile security; • understand the security architecture and threat model of mobile networks; • explain the security models of popular mobile operating systems, applications, and services; • analyze the threats to popular mobile operating systems, applications, and services; • develop practical skills to detect attacks, to assess the security risk of mobile applications and services, and to analyze mobile malware.
Intended Learning Outcomes *(Note 1)*	Upon completion of the subject, students will be able to: Professional/academic knowledge and skills (a) understand the security architectures of cellular networks and WiFi networks along with the major threats in mobile communication; (b) explain the security model of the Android system, iOS systems, and their applications; (c) analyze Android applications, evaluate the threats to them, and dissect malware; (d) identify major security and privacy issues in popular mobile services and applications. Attributes for all-roundedness (e) acquire critical thinking and analytical skills, and improve technical writing as well as presentation skills.

Subject Synopsis/ Indicative Syllabus

(Note 2)

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

Teaching/Learning Methodology

(Note 3)

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

(Note 4)

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)						
		a	b	c	d	e		
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:	
▪ Lecture	26 Hrs.
▪ Tutorial/Lab/Workshop	13 Hrs.
Other student study effort:	
▪ Assignment + Term project	40 Hrs.
▪ Self-study + Examination preparation	39 Hrs.
Total student study effort	118 Hrs.

Reading List and References

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

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

3. Himanshu Dwivedi, Chris Clark, and David Thiel, Mobile Application Security, McGraw-Hill Osborne Media, 2010.

4. Charlie Miller, Dion Blazakis, Dino DaiZovi, Stefan Esser, Vincenzo

	Iozzo, Ralf-Philipp Weinmann, iOS Hacker's Handbook, Wiley, 2012 5. Patrick Traynor, Patrick McDaniel, and Thomas La Porta, Security for Telecommunications Networks, Springer, 2008. 6. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002. 7. Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, and Valtteri Niemi, LTE Security, Wiley, 2012. 8. Levente Buttyán and Jean-Pierre Hubaux, 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