Subject Description Form

Subject Code	COMP5580
Subject Title	Mobile and Wireless Security
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	To equip students with a foundational understanding of mobile and wireless security and practical skills for handling security issues in mobile systems and 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 systems, apps, and services; • analyse threats to popular mobile systems, apps, and services; • develop practical skills to detect attacks, assess the security risk of mobile systems, apps and services, and analyse mobile malware.
Intended Learning Outcomes	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, and acquire practical skills to identify the major threats to mobile communication; b. analyse the security models of Android, iOS, and OpenHarmony systems, along with their apps and services; c. evaluate the security issues in popular mobile systems, apps, and services, and dissect malware; *Attributes for all-roundedness* d. deal with complex ethical and professional issues through critical thinking and analytical skills, and improve technical writing as well as presentation skills; e. demonstrate leadership and qualities of reflective practitioners.
Subject Synopsis/ Indicative Syllabus	1. Overview of mobile communication and its security (e.g., mobile communication concepts, types of attacks, basic cryptography). 2. Cellular networks security (e.g., access control and authentication in cellular networks). 3. WiFi network security (e.g., WiFi network attacks). 4. Android security (e.g., Android system, Android security model, app analysis, app reverse engineering). 5. iOS security (e.g., iOS system, iOS security model, app analysis). 6. OpenHarmony security (e.g., OpenHarmony system and security model, app analysis). 7. Mobile malware (e.g., taxonomy, malware detection). 8. Selected topics on mobile security (e.g., NFC security).

<table>
<tr><td>Teaching/Learning Methodology</td><td>The course will be delivered as a combination of lectures, tutorials, labs, and a class project. It will emphasise on both the principles and practices of mobile and wireless security. The principles will be covered mainly through lectures and tutorials, while the practical aspects will be taught through labs. The class project will help students reinforce what they have learned, including both principles and practical skills.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="5">Intended subject learning outcomes to be assessed (Please tick as appropriate)</td></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td></tr>
<tr><td>1. Assignment</td><td>10</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>2. Class Project</td><td>20</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>3. Final Exam</td><td>70</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>
</table>

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:
Continuous assessments consist of assignments and a class project, which are designed to help students achieve the intended learning outcomes. Although tutorials and labs are not assigned an assessment weighting, they are designed to encourage students to acquire a deep understanding of the relevant knowledge.
The final exam will evaluate student’s understanding and practical skills regarding security issues in mobile systems, networks, apps, and services.</td></tr>
<tr><td>Student Study Effort Expected</td><td>
<table>
<tr><td>Class contact:</td><td></td></tr>
<tr><td>▪ Lecture</td><td>26 Hrs.</td></tr>
<tr><td>▪ Tutorial/Lab</td><td>13 Hrs.</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>▪ Assignment and Class Project</td><td>40 Hrs.</td></tr>
<tr><td>▪ Self-Study and Examination Preparation</td><td>39 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>118 Hrs.</td></tr>
</table>
</td></tr>
<tr><td>Reading List and References</td><td>1. Au, M.-H., & Choo, R. K.-K. (Eds.). (2017). Mobile Security and Privacy: Advances, Challenges and Future Research Directions. Elsevier.
2. Doherty, J. (2021). Wireless and Mobile Device Security (Second Edition). Jones & Bartlett Learning.
3. Khari, M., Bharti, M., & Niranjanamurthy, M. (Eds.). (2023). Wireless Communication Security: Mobile and Network Security Protocols. Wiley-Scrivener.
4. Osterhage, W. (2018). Wireless Network Security (Second edition.). CRC Press.
5. Garg, S., & Baliyan, N. (2024). Mobile OS Vulnerabilities: Quantitative and Qualitative Analysis. CRC Press.
6. Chell, D. (2015). The Mobile Application Hacker’s Handbook. Wiley.
7. Proceedings of IEEE Symposium on Security and Privacy.
8. Proceedings of USENIX Security Symposium.</td></tr>
</table>

	9. Proceedings of ISOC Network and Distributed System Security Symposium. 10. Proceedings of ACM Conference on Computer and Communications Security. 11. Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks. 12. Proceedings of European Symposium on Research in Computer Security. 13. Proceedings of International Symposium on Research in Attacks, Intrusions and Defenses. 14. Proceedings of Annual Computer Security Applications Conference.