Subject Description Form

Subject Code	EIE4113
Subject Title	Wireless and Mobile Systems
Credit Value	3
Level	4
Pre-requisite	For 42480 EIE3120 Network Technologies and Security For 42470 EIE3333 Data and Computer Communications
Exclusion	Mobile Networking (EIE4104)
Objectives	This subject aims to provide students with an understanding of various security concerns in wireless networks (e.g., WiFi and mobile cellular networks) and mobile systems and applications (e.g., Android and iOS).
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand the security threats, concerns, and vulnerabilities in wireless and mobile systems, and the corresponding security mechanisms and authentication procedures 2. Understand the strategies for developing secure mobile applications, and the use of mobile security penetration tools for evaluating the robustness of mobile applications 3. Apply the knowledge to develop practical applications that are robust against mobile platform attack tools Category B: Attributes for all-roundedness 4. Understand the creative process when designing solutions to a problem
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Introduction to Mobile and Wireless Networks Mobile cellular networks (3G/4G LTE), IEEE wireless networks (IEEE 802.11, IEEE 802.15), mobile networks (NEMO, MANET). 2. Vulnerability of Wireless Networks Threats and risks to telecommunication systems, vulnerabilities from wired to wireless communications, fundamental security mechanisms. 3. WiFi Security Attacks on wireless networks, security in the IEEE 802.11 standard, security in 802.11i, authentication in wireless networks, layer 3 security mechanisms. 4. Security in Mobile Telecommunication Networks Vulnerability of signaling systems, GSM and GPRS security, 3G security, network interconnection. 5. Mobile Systems and Development Strategies Top issues facing mobile devices, tips for secure mobile application development, mobile HTML security, SMS security, mobile geolocation. 6. Android and iOS Security Android IPC mechanisms, security model, permission review, security tools. iOS security testing, application format, permissions and user controls.

Mobile security penetration testing tools.

Teaching/Learning Methodology

Lectures: The subject matters will be delivered through lectures. Students will be engaged in the lectures through Q&A, discussions and specially designed classroom activities.

Tutorials: During tutorials, students will work on/discuss some chosen topics in small group. This will help strengthen the knowledge taught in lectures.

Laboratory and assignments: During laboratory exercises, students will perform hands-on tasks to practice what they have learned. They will evaluate the vulnerability of systems and design solutions to problems. The assignments will help students to review the knowledge taught in class.
While lectures and tutorials will help to achieve the professional outcomes, the open-ended questions in laboratory exercises and assignments will provide the chance to students to exercise their creativity in problem solving.

Assessment Methods in Alignment with Intended Subject Learning Outcomes

Specific Assessment Methods/Tasks	**% Weighting**	**Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)**			
		1	**2**	**3**	**4**
1. Continuous Assessment	(50%)				
• Homework and assignments	10%	✓	✓	✓	✓
• Tests	10%	✓	✓		
• Laboratory exercises	30%			✓	✓
2. Examination	50%	✓	✓		✓
Total:	100%				

Student Study Effort Expected

Class contact (time-tabled):	
• Lecture	24 Hours
• Tutorial/Laboratory/Practice Classes	15 Hours
Other student study effort:	
• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination	36 Hours
• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing	30 Hours
Total student study effort:	**105 Hours**

Reading List and References

Reference Books:

1. H Chaouchi, M Laurent-Maknavicius, *Wireless and Mobile Network Security*, Wiley, 2009.
2. P. Venkataram, B. Sathish Babu, *Wireless and Mobile Network Security*, Tata McGraw-Hill, 2010.
3. H. Dwivedi, C. Clark, D. Thiel, *Mobile Application Security*, McGraw-Hill, 2010.

Last Updated	November 2014
Prepared by	Dr Ivan Ho