Secure Software Engineering

Module Information

2022.01, Approved

Summary Information

Module Code	7138COMP
Formal Module Title	Secure Software Engineering
Owning School	Computer Science and Mathematics
Career	Postgraduate Taught
Credits	20
Academic level	FHEQ Level 7
Grading Schema	50

Teaching Responsibility

LJMU Schools involved in Delivery
Computer Science and Mathematics

Learning Methods

Learning Method Type	Hours
Lecture	12
Practical	24

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
JAN-CTY	CTY	January	12 Weeks

Aims and Outcomes

Aims	To develop students' analysis skills in identifying and understanding security problems and vulnerabilities, and the methods, tools, and techniques that can be used during software development to prevent them.To develop students software development skills by applying a software development lifecycle in order to improve software security and robustness.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Apply best-practice security architectures and patterns to mitigate threats against software in different environments.
MLO2	2	Demonstrate a comprehensive understanding of applying security techniques to software development.
MLO3	3	Show critical awareness of the complexity of contemporary software vulnerabilities and the techniques to discover and mitigate them.

Module Content

Outline Syllabus	-Characteristics of large-scale software systems projects, team membership and activities.-Networking vulnerabilities, access control, random number generation, cryptography, and authentication in software development.-Understanding, exploiting, and mitigating common software vulnerabilities.-Testing software to discover security vulnerabilities.-Process models and lifecycles for secure software development.-Threat modelling and formal techniques for vulnerability analysis.-Secure deployment and post-deployment management of software.-Understanding the implications of different computing environments on security and the software development process.-Programming languages and security characteristics, decompilation, disassembly, and obfuscation.-Recent examples from computing are used throughout and practical exercises used to illustrate the applications of these concepts.
Module Overview	This module will develop your skills in identifying and understanding security problems and vulnerabilities. You will explore the methods, tools, and techniques that can be used to prevent them. You will gain software development skills by applying a software development lifecycle to improve security and robustness. You will work in small teams, mimicking the environment in which professional software engineers work.
Additional Information	This module is intended to expose students to development practices that lead to reliable and secure software. Design models (secure development lifecycle model) as well technical skills including code vulnerability detection and testing will be explored. Students would benefit from prior programming experience but it is not essential as some experience will be gained during semester 1 modules, and extra tutorial support will be provided within the module. Students will work in small teams, mimicking the environment that most professional software engineers work in.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Technology	Software testing and security	100	0	MLO1, MLO2, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Nathan Shone	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings