Computer Security

Module Information

2022.01, Approved

Summary Information

Module Code	7506YPCM
Formal Module Title	Computer Security
Owning School	Civil Engineering and Built Environment
Career	Postgraduate Taught
Credits	10
Academic level	FHEQ Level 7
Grading Schema	50

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
YPC International College (Kolej Antarabangsa YPC)

Learning Methods

Learning Method Type	Hours
Lecture	11
Practical	11
Tutorial	11

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
SEP-PAR	PAR	September	12 Weeks

Aims and Outcomes

Aims	To develop the knowledge of various security threats and vulnerabilities in computer systems as well as the importance of computer security. To critically assess a variety of generic security technologies for protection of computer systems.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Identify and analyse security threats and vulnerabilities, and assess their impacts on given computer applications.
MLO2	2	Evaluate and specify requirements for countering security threats identified for given applications.
MLO3	3	Critically analyse security techniques and tools to develop appropriate security mechanisms and solutions for protection of computer systems.
MLO4	4	Critically analyse current research issues and application in computer security.

Module Content

Outline Syllabus	Fundamentals Of Computer Security – Security Concepts: Confidentiality, Integrity, Availability and Security Policies. Security Problems: Security Breaches and Vulnerabilities. Information Encryption And Decryption: Terminology, Systems and Applications. Risk Analysis And Security Management: Principles, Techniques, Processes and Standards. Personal Computer Security – Security Problems. Security Measures: File Protection And Password Selection Criteria. Computer Attacks: Examples, Sources And Prevention. Secure Operating Systems: Security Models And Design Issues. Network Security – Threats To Computer Networks. Network Security Countermeasures: Firewalls And Intrusion Detection Systems. Mobile Phone Security, Wireless Security: Vulnerabilities, Security Services And Protocols In The Wireless Environment.Encryption And Decryption – Crypto Key Management: Protocols And Services. Digital Signatures: Importance And Methods. Authentication: Principles, Protocols And Services. Network Access Controls: Policies And Mechanisms. Security Applications: Secure Electronic Payment Protocols. Database Security: Data Classification. Security Requirements: Integrity, Authentication And Authorization. Techniques For Multi-level Security: Access Control Models, Data Encryption And Architectures.
Module Overview	
Additional Information	This advanced course is intended for post-graduate students interested in the field of computer security. The purpose of the course is to provide the fundamental technical concepts and research issues essential for computer security. This module develops the understanding of threats and the security requirements of computer systems, as well as tools and techniques to enforce security.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Essay	ESSAY 2,500 words	50	0	MLO1, MLO4
Artefacts	ARTEFACT 2,500 words	50	0	MLO2, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Bob Askwith	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings