Network Defence

Module Information

2022.01, Approved

Summary Information

Module Code	6213COMP
Formal Module Title	Network Defence
Owning School	Computer Science and Mathematics
Career	Undergraduate
Credits	20
Academic level	FHEQ Level 6
Grading Schema	40

Teaching Responsibility

LJMU Schools involved in Delivery
Computer Science and Mathematics

Learning Methods

Learning Method Type	Hours
Lecture	22
Tutorial	22

Module Offering(s)

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

Aims and Outcomes

Aims	To gain a significant understanding of various security vulnerabilities in and cyber threats to computer systems and applications.To convey the importance of cyber security and network defence. To experience a variety of security technologies for protection of computer devices/systems/networks.To promote the use of appropriate methodologies and tools in the analysis, design, implementation of secure systems.To examine current research issues in computer security and network defence.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Critically evaluate the threats and vulnerabilities to information, computing and communications systems.
MLO2	2	Design and develop security countermeasures for computing applications.
MLO3	3	Critically assess the use of information security management techniques.

Module Content

Outline Syllabus	The spectacular growth of the Internet has spawned a great demand for awareness of security threats to computer networks and application of security techniques to network protection. In response to the demand, this module examines various security issues and solutions to computer and network protection. Throughout the academic year, the syllabus material will cover:-Computer security background; security goals, problems, models.-Fundamental security design principles: OSI architecture, levels of security impact, threat modelling (STRIDE and DREAD).-Network security: network characteristics and topologies, vulnerabilities and attacks, OSI model – security issues, attacks, threats, security control.-System security - technologies including firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, anti-viruses, access controls.-Malicious software: malware propagation, payload, countermeasures.-Securing devices and network from attack; safe use of the Internet, the Internet of Things (IoT), defence-in-depth, social engineering, system hardening.-Access control: importance, principles, Bell-LaPadula, Chinese wall, Biba model. -Cryptographic techniques: algorithms, protocols, authentication, key management and public key infrastructures. -Introducing security research topics; e.g. advanced persistent threats, trusted computing, IoT security and privacy concerns, big data.
Module Overview	This module aims to develop your understanding of computer security and network defence. Through critically assessing a variety of security technologies for protection of computer networks, you will develop practical skills in the use of security countermeasure technologies and associated tools.
Additional Information	This module aims to develop an understanding of computer security and network defence. Through assessing critically a variety of security technologies for protection of computer networks, students will develop practical skills in the use of security countermeasure technologies and associated tools.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Network security scenario	40	0	MLO1, MLO2
Centralised Exam	Examination	60	2	MLO1, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Aine Mac Dermott	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings