Computer Security

Module Information

2022.01, Approved

Summary Information

Module Code	7131COMP
Formal Module Title	Computer Security
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	11
Practical	11
Tutorial	11

Module Offering(s)

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

Aims and Outcomes

Aims	To develop an understanding of Computer Security and to understand security threats and vulnerabilities to information, computing and communications systems.To critically assess 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.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Critically review current research issues and developments in computer security
MLO2	2	Critically evaluate a complex computer security problem
MLO3	3	Apply complex skills relating to security techniques and tools to secure a computer system.

Module Content

Outline Syllabus	Computer security background; security goals, design and principles, problems, models.Security services: authentication, key management and PKI.Security technologies including firewalls, intrusion detection systems, intrusion prevention systems, biometrics, anti-viruses, access controls, administrative security and database management.Malware: viruses and worms, botnets, ransomware, spyware.Securing devices and network from attack; safe use of the Internet, the Internet of Things (IoT), defence-in-depth.Access control: importance, principles, Bell-LaPadula, Chinese Wall, Biba.Cryptographic techniques: algorithms, protocols, authentication, key management and PKI.Introducing security research topics; e.g. advanced persistent threats, trusted computing, composition, digital rights, IoT security and privacy concerns, big data.
Module Overview	The purpose of the module is to provide the fundamental technical concepts and research issues essential for computer security. This module develops the understanding of threats to and the security requirements of computer systems, as well as tools and techniques to enforce security. It aims to: develop the knowledge of various security threats and vulnerabilities in computer systems as well as the importance of Computer Security critically assess a variety of generic security technologies for the protection of computer systems promote the use of appropriate methodologies and tools in the analysis, design, implementation and management of secure systems examine current research issues in Computer Security
Additional Information	This advanced course is intended for postgraduate 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 to 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

Report	Security Research Report	40	0	MLO1
Report	Practical Security Solution	60	0	MLO2, MLO3

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Kellyann Stamp	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings