Network Security

Module Information

2022.01, Approved

Summary Information

Module Code	7133COMP
Formal Module Title	Network 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
JAN-CTY	CTY	January	12 Weeks

Aims and Outcomes

Aims	To develop an understanding of various security vulnerabilities in and threats to computer networks as well as the importance of network security.To assess critically a variety of generic security technologies for protection of computer networks.To promote the use of appropriate security techniques to solve network security problems.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Demonstrate critical awareness of network security threats and vulnerabilities
MLO2	2	Apply security analysis skills to complex security problems for a given application.
MLO3	3	Critically evaluate security protocols and mechanisms for the provision of security services needed for secure networked applications.
MLO4	4	Demonstrate comprehensive understanding of security techniques to solve network security problems.

Module Content

Outline Syllabus	Fundamentals of network security: security concepts, security policies, security threats and vulnerabilities, authentication principles and means, trust management, and importance of network security and its applications.Cryptographic techniques: cryptanalytic attacks, conventional/symmetric cryptography (e.g. DES), public-key/asymmetric cryptography (e.g. RSA), cryptographic key distribution, key establishment, hash functions (e.g. SHA), message authentication code and digital signatures (e.g. DSA).Security measures: message integrity, message confidentiality, user and message authentication, public-key certification, key certificate validation and revocation, and X.509 directory authentication services.Network security applications: network-based authentication protocols and services (e.g. Kerberos), IP security (e.g. IPSec) for secure Internet-based communications, virtual private networks, web security (e.g. SSL/TLS), e-mail security (e.g. PGP), and wireless security.
Module Overview	The growth of the Internet means that it is more important than ever to be aware of security threats to computer networks. This module explores security vulnerabilities and threats, emphasising the importance of network security. It looks at security issues and solutions to network protection, critically assessing security technologies and promoting the use of security techniques.
Additional Information	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 network protection.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Artefacts	Design and analysis	40	0	MLO2, MLO3
Centralised Exam	Examination	60	2	MLO1, MLO4

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Qi Shi	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings