Liverpool John Moores University

Title:	NETWORK SECURITY
Status:	Definitive
Code:	**7133COMP** (122201)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Qi Shi	Y
Robert Askwith	

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	35
Total Learning Hours:	200	**Private Study:**	165		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	11
Practical	11
Tutorial	11

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Group Assessment - Design and analysis of security solutions for the protection of a selected networked application.	40	
Exam	AS2	Examination.	60	2

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.

Learning Outcomes

After completing the module the student should be able to:

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

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Design and analysis	2	3
Examination	1	4

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.

Learning Activities

Include attending lectures and tutorials, as well as reading books and handouts.

Notes

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.