Liverpool John Moores University

Title:	NETWORK SECURITY
Status:	Definitive
Code:	**7077COMP** (120335)
Version Start Date:	01-08-2014
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
Qi Shi	Y

Academic Level:	FHEQ7	**Credit Value:**	20.00	**Total Delivered Hours:**	38.00
Total Learning Hours:	200	**Private Study:**	162		

Delivery Options
Course typically offered: Semester 2

Component	Contact Hours
Lecture	12.000
Practical	12.000
Tutorial	12.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Design and analysis of security solutions for the protection of a selected networked application.	40.0	
Exam	AS2	Examination.	60.0	2.00

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	Explain a variety of generic security threats and vulnerabilities.
2	Identify and analyse particular security problems for a given application.
3	Demonstrate advanced knowledge of security protocols and mechanisms for the provision of security services needed for secure networked applications.
4	Apply appropriate 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.

References

Course Material	Book

Author	Stallings, W.
Publishing Year	2013
Title	Network Security Essentials
Subtitle	Applications and Standards
Edition	5th Edition
Publisher	Prentice Hall
ISBN	0133370437

Course Material	Book
Author	Stallings, W.
Publishing Year	2013
Title	Cryptography and Network Security
Subtitle	Principles and Practice
Edition	6th Edition
Publisher	Prentice Hall
ISBN	0133354695

Course Material	Book
Author	Pfleeger, C. & Pfleeger, S.
Publishing Year	2007
Title	Security in Computing
Subtitle	
Edition	4th Edition
Publisher	Prentice Hall
ISBN	0132390779

Course Material	Journal / Article
Author	
Publishing Year	
Title	ACM Conference on Computer and Communications Security, IEEE Symposium on Security and Privacy, and Applied Computer Security Applications Conference
Subtitle	
Edition	
Publisher	
ISBN	

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.