Liverpool John Moores University

Title:	NETWORK SECURITY
Status:	Definitive
Code:	**6066COMP** (117752)
Version Start Date:	01-08-2019
Owning School/Faculty:	Computer Science
Teaching School/Faculty:	Computer Science

Team	Leader
Qi Shi	Y
Aine MacDermott	

Academic Level:	FHEQ6	**Credit Value:**	24	**Total Delivered Hours:**	74
Total Learning Hours:	240	**Private Study:**	166		

Delivery Options
Course typically offered: Standard Year Long

Component	Contact Hours
Lecture	24
Practical	12
Seminar	12
Tutorial	24

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Develop a solution to a given network security scenario.	50	
Exam	AS2	Examination	50	2

Aims

Understand security threats and vulnerabilities to information, computing and communications systems.
Assess critically a variety of generic security technologies for protection of computer

networks.
Develop practical skills in the use of security countermeasure technologies and associated tools.

Learning Outcomes

After completing the module the student should be able to:

1	Critically evaluate the threats and vulnerabilities to information, computing and communications systems.
2	Critically review use of security countermeasures in a computing environment.
3	Critically evaluate the use of information security management techniques.
4	Apply creative skills in the development of security software and cryptographic mechanisms and protocols to mitigate these threats and vulnerabilities.

Learning Outcomes of Assessments

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

Network security solution	2	3
Examination	1	4

Outline Syllabus

Computer security background; security goals, problems, models.
Cryptographic techniques: conventional cryptography (e.g. AES), public-key cryptography (e.g. RSA), digital signatures (e.g. DSA), and applications of cryptography.
Security services: authentication, key management and PKI, Kerberos.
Security technologies including firewalls, intrusion detection systems, biometrics, anti- viruses, access controls.
Malware; viruses and worms, botnets, mobile code security.
Securing the personal computer and network from attack; safe use of the Internet and Web.
Network security protocols: IP security (e.g. IPSec), web security (e.g. SSL/TLS), e-mail security, and e-payment systems (e.g. SET).
Access control: Bell-LaPadula, Chinese Wall, Biba.
Security management: policies, risk assessment, legal considerations, privacy, ethics, standards, education.
Introducing security research topics; e.g. trusted computing, composition, digital rights.

Learning Activities

Lectures and practical work.

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 computer and network protection.