Liverpool John Moores University

Title:	Network Defence
Status:	Definitive
Code:	**6213COMP** (128014)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Aine MacDermott	Y
Alex Akinbi	
Nathan Shone	

Academic Level:	FHEQ6	**Credit Value:**	20	**Total Delivered Hours:**	46
Total Learning Hours:	200	**Private Study:**	154		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	22
Tutorial	22

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Network security scenario	40	
Exam	AS2	Examination	60	2

Aims

To gain a significant understanding of various security vulnerabilities in and cyber threats to computer systems and applications.
To convey the importance of cyber security and network defence. To experience 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 and network defence.

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	Design and develop security countermeasures for computing applications.
3	Critically assess the use of information security management techniques.

Learning Outcomes of Assessments

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

Network security scenario	1	2
Examination	1	3

Outline Syllabus

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.
Throughout the academic year, the syllabus material will cover:
-Computer security background; security goals, problems, models.
-Fundamental security design principles: OSI architecture, levels of security impact, threat modelling (STRIDE and DREAD).
-Network security: network characteristics and topologies, vulnerabilities and attacks, OSI model – security issues, attacks, threats, security control.
-System security - technologies including firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, anti-viruses, access controls.
-Malicious software: malware propagation, payload, countermeasures.
-Securing devices and network from attack; safe use of the Internet, the Internet of Things (IoT), defense-in-depth, social engineering, system hardening.
-Access control: importance, principles, Bell-LaPadula, Chinese wall, Biba model.
-Cryptographic techniques: algorithms, protocols, authentication, key management and public key infrastructures.
-Introducing security research topics; e.g. advanced persistent threats, trusted computing, IoT security and privacy concerns, big data.

Learning Activities

Attending lectures, practical sessions and tutorials, reading academic papers and online resources as advised.

Notes

This module aims to develop an understanding of computer security and network defence. Through assessing critically a variety of security technologies for protection of computer networks, students will develop practical skills in the use of security countermeasure technologies and associated tools.