Liverpool John Moores University

Title:	COMPUTER SECURITY
Status:	Definitive
Code:	**7131COMP** (122199)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Kellyann Stamp	Y
Aine MacDermott	
Robert Askwith	

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	33
Total Learning Hours:	200	**Private Study:**	167		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	11
Practical	11
Tutorial	11

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Research a solution for a contemporary computer security problem.	40	
Artefacts	AS2	Develop a solution to a computer security problem	60	

Aims

To develop an understanding of Computer Security and to understand security threats and vulnerabilities to information, computing and communications systems.

To critically assess 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.

Learning Outcomes

After completing the module the student should be able to:

1	Critically review current research issues and developments in computer security
2	Critically evaluate a complex computer security problem
3	Apply complex skills relating to security techniques and tools to secure a computer system.

Learning Outcomes of Assessments

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

Security Research Report	1	
Practical Security Solution	2	3

Outline Syllabus

Computer security background; security goals, design and principles, problems, models.
Security services: authentication, key management and PKI.
Security technologies including firewalls, intrusion detection systems, intrusion prevention systems, biometrics, anti-viruses, access controls, administrative security and database management.
Malware: viruses and worms, botnets, ransomware, spyware.
Securing devices and network from attack; safe use of the Internet, the Internet of Things (IoT), defense-in-depth.
Access control: importance, principles, Bell-LaPadula, Chinese Wall, Biba.
Cryptographic techniques: algorithms, protocols, authentication, key management and PKI.
Introducing security research topics; e.g. advanced persistent threats, trusted computing, composition, digital rights, IoT security and privacy concerns, big data.

Learning Activities

Lectures, practical lab exercises, tutorials and advanced individual research. The individual research builds on core computer security concepts covered in the lectures through reading academic material, journals, and conference papers in the area of computer security.

Notes

This advanced course is intended for postgraduate students interested in the field of computer security. The purpose of the course is to provide the fundamental technical concepts and research issues essential for computer security. This module develops the understanding of threats to and the security requirements of computer systems, as well as tools and techniques to enforce security.