Module Title	**Systems and Cyber Security**
Level	6
Reference No.	CSI_6_SCS
Credits	20
Student Study Hours	Total: 200 Contact hours: 52 Student managed learning hours: 148
Pre-Requisites	None
Co-requisites	None
Excluded combinations	None
Module coordinator	TBC
Division	Division of Computer Science and Informatics
Short Description	This module covers all aspects of the complex field of security in computer systems and networks. It will teach the fundamental principles of computer security and how they impact the many different areas in which computer technology is used. It will explore the diverse range of threats faced by systems and the network infrastructure that connect them together and the measures that can be taken to counter them.
Aims	This module aims to make students aware of security issues in all fields of computing and provide a clear understanding of best practice and risk mitigation techniques. Students will acquire knowledge of real and current threats and by studying the underlying principles be prepared to understand new threats that will arise in future.
Learning Outcomes	**LO1: Knowledge and Understanding** ● Appraise the fundamental issues related to security, the exploits that can undermine security and the preventative measures that are possible. **LO2: Intellectual Skills** ● Clearly reason about the origins and reasons for vulnerabilities in systems and know how to avoid them. (Maps to: BCS 2.2.1 a1-a5, a7-a9; 2.2.3 a1-a3) **LO3: Practical Skills** ● Analyse systems for security weaknesses and propose mitigating measures that could be taken. (Maps to: BCS 2.2.1 b1-b4; 2.2.3 a4-a6) **LO4: Transferable Skills** ● Evaluate potential risks associated with the technological systems in use in every sphere of human activity. (Maps to: BCS 2.2.1 c1-c2)
Employability	As computer technology becomes ever more deeply embedded into all aspects of society, its potential for abuse becomes ever more serious. Computer security is a field which is becoming more and more vital, in commerce and businesses of all kinds, for political and military applications and simply in one's personal life. The need for expertise in this area will continue to increase for the foreseeable future, and employers of all kinds will be seeking individuals who have it.
Teaching and Learning Pattern	The module will be delivered using a combination of lecture/seminar sessions and computer lab/workshop sessions. The lecture/seminars will consist of the delivery, discussion and intellectual investigation of factual and conceptual material. The laboratory sessions will consist of practical exercises using relevant technologies and provide opportunities for students to develop their understanding through independent experimentation.
Indicative Content	● Concepts of risk, threats, vulnerabilities, and attack vectors ● The principle of least privilege and isolation ● Use of cryptography for data and network security ● Attack motivations; crime, espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats

	● Network specific threats; denial of service, spoofing, sniffing and traffic redirection, man-in-the-middle, message integrity attacks, routing attacks, and traffic analysis ● Malware; viruses, worms, spyware, botnets, Trojan horses or rootkits ● Applied psychology and security policies ● Biometric authentication ● Defensive Programming; Input validation and data sanitization, buffer overflows, integer errors, SQL injection; XSS vulnerability ● Web security; same-origin policy; session management, authentication; HTTPS and certificates
Assessment *Elements and weightings*	**EXAM 40% : COURSEWORK 60%** **Summative Assessment** Exam: 2hr paper covering topics from a selection of areas from the module content. (LO1-LO3) Coursework: Likely to be in a form of an individually assessed practical exercise involving the analysis of the data from investigation tools and a written report analysing a security scenario and including recommendations based on evidence identified in the scenario. (LO1,LO2, LO4) **Formative Assessment** Skills for the summative assessment will be embedded throughout formative opportunities in Lectures and Workshops. Formative assessment will take different forms, such as: ● think-pair-share concept and class discussions ● verbal feedback on tutorial activities ● observation and questioning to provide instant feedback as the student takes part in learning activities
Indicative Sources *(Reading lists)*	**Core:** There is no core textbook defined for this module. Students are expected to refer to the indicative sources below: **Optional:** ● Donaldson, S. et al (2018) *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, Apress; 2015 edition. ISBN-10: 1430260823 ● Mowbray, T.J. (2013) *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions* John Wiley & Sons; 1st edition. ISBN-10: 1118697111