Module Title	**Systems - Cyber Threats, Vulnerabilities and Countermeasures**
Level	7
Reference No. *(showing level)*	CSI_7_SYS
Credit Value	20
Student Study Hours	Total: 200 Contact hours: 52 Student managed learning hours: 148 Requirements for Self-Managed Learning Hours: • Read research papers and make notes for seminar presentations. • Undertake research work, complete and write up lab exercises and assessments. • Maintain a journal on contemporary research and technical work.
Pre-requisite learning	None
Co-requisites	None
Excluded combinations	None
Module co-ordinator	TBC
School/Division	Engineering/Computer Science and Informatics
Short Description	.
Aims	To develop an in-depth, critically evaluative knowledge of concepts of security in networks and systems and the acquisition of knowledge about the processes, techniques, and security technologies to achieve an end-to-end security system. The course will analyse the security requirements and the vulnerabilities that threaten the smooth functioning of a computer system / network and will inform about ways of prevention, protection, recognition, and treatment of malicious attacks using appropriate technologies and security tools.
Learning Outcomes	**Knowledge and Understanding**: 1. Demonstrate a systematic understanding of security threats-vulnerabilities and practical experience in designing remedies and mechanisms against vulnerabilities-attacks/technologies, their architecture including the importance of research, methodologies, driving innovation and contribution; (covers course outcomes: a1, a2; BCS requirements: 7.1.1 - 7.1.4; 8.1.1 - 8.1.2; 8.2.1; 9.1.1, 9.1.2, 9.2.2; 10.1.1, 10.1.2, 10.2.1) 2. Consistently produce and review research informed work which applies and is at the forefront of the developments in the domain of attacks and vulnerabilities in heterogeneous systems (e.g., wireless networks, IoT, Cloud, application servers) and contribute to the design of mechanisms to protect the systems; (covers course outcomes: a3; BCS requirements: 7.1.1, 7.1.4, 7.1.6; 8.1.1 - 8.2.1; 9.1.1 - 9.1.3) 3. Study and management of associated projects including timescales, risk identification/management, cost and quality constraints, as well as ethics working within professional frameworks and social/legal constraints (covers course outcomes: a4; BCS requirements: 7.1.5 - 7.1.9; 8.1.1 - 8.2.2 9.1.3 - 9.2.3; 10.1.1 - 10.2.3) Intellectual Skills: • Conduct a critically evaluative analysis of a Cyber Security case-based domain in order to design, develop and evaluate techniques and security technology solutions; also developing the in-depth

	knowledge necessary to identify and apply suitable techniques in order to synthesize advanced theory/practical concepts. (covers course outcomes: b1, b2; BCS requirements: 8.1.1 - 8.1.3; 9.1.1 - 9.1.3; 10.1.1 - 10.1.3) • Specify/critically evaluate a Cyber Security project applying appropriate techniques to protect systems against attacks either at the protocol level or at the system level, also evaluate life-cycle/methodologies; conducting effective independent research (covers course outcomes: b3, b4; BCS requirements: 8.1.1 - 8.1.3; 9.1.1 - 9.1.3; 10.1.1 - 10.1.3) **Practical Skills:** • Develop the in-depth knowledge necessary for enhancing security in networks and systems project domains and apply suitable techniques in order to synthesize advanced (theory/practical) concepts to design, develop, deploy, and maintain bespoke/innovative solutions; as well as being able to specify, manage, critically evaluate a project applying appropriate technology, techniques, life-cycle/methodology. (covers course outcomes: c2, c4; BCS requirements: 8.2.1, 8.2.1; 9.2.1 - 9.2.3; 10.2.1 - 10.2.3) • Be able to assess the application of techniques and security technologies for practical solving security problems in networks and information systems making concise, engaging and well-structured oral presentations, arguments and explanations; Communication /presentation of semantic web and mobile projects and concepts to a wide range of audiences. (covers course outcomes: c1, c3; BCS requirements: 8.2.1, 8.2.1; 9.1.1 - 9.2.3; 10.2.1 - 10.2.2) **Transferable Skills:** • Critically evaluate existing/emerging Cyber Security technology and techniques, carrying out independent research, recognize and contribute to opportunities for innovation, deal with uncertainty, evaluate and manage risks, synthesise ideas/theories/solutions and report back appropriately to your peers, also conducting effective peer reviews. (covers course outcomes: d2, d3; BCS requirements: 7.1.1 - 7.1.4) • Self-manage your study time and work effectively to meet deadlines, select and evaluate appropriate knowledge, skills, etc...; also select and evaluate supporting resources/tools for a particular purpose, as well as being able to make effective contributions as team member/leader when required. (covers course outcomes: d1, d4; BCS requirements: 7.1.5 - 7.1.9) .
Employability skills	There is a constant commercial need/demand for System and Cyber in cutting-edge systems such as wireless network, IoT, Cloud and application servers. The module delivers skills in these areas that are directly relevant in both commercial and research environments.
Teaching and learning pattern	All module teaching and learning content will be hosted on the University VLE giving constant access to all material maximising your learning potential. Weekly lectures will present fundamental topics and knowledge in the subject area. Lectures may feature presentations, Audio-Visual Media and Digital Content as appropriate. Guest lecturers may also be used where appropriate. Although a traditional single semester-based delivery mode is assumed, the module may also be provided in an intensive study/block mode 5-day delivery for short courses.
Supporting Tutorials	For each lecture an accompanying tutorial (also hosted on the VLE site) will provide the opportunity where possible to practice the design, software engineering and maintenance of practical solutions to problem domains. Practical exercises will focus on the application of industry standard techniques and tools using large real-world data sets where appropriate.

Indicative content	• Security threats and vulnerabilities in different networking environments. • Security policies & Risk Management • Attacks, vulnerabilities, and tools for attack detection-protection • Protocol vulnerabilities and remedies • Security mechanisms for OS • Security in wireless systems • Security in Information Systems • Use Case Studies
Assessment *Elements and weightings*	**Summative Assessment** • Programming assignment 1: **Final submission length: 2000 words (40% of coursework total)** The is to gain experience with an security tool suite (openVPN, openSSL, snort) • Programming assignment 2: **Final submission length: 3000 words (60% of coursework total)** The aim of this assignment is to exploit vulnerabilities in an environment (network, cloud, protocol) (covers module outcomes: a1-a3, b1-b2, c1-c2, d1-d2; BCS requirements: 7.1.5, 8.2.1, 8.2.1; 9.2.1 - 9.2.3; 10.2.1 - 10.2.3) (**Formative Assessments:** The students will usually be given a range of weekly tutorial-based tasks (both individual/group work) comprised of formative exercises imparting the knowledge and skills required to satisfy the learning outcomes)
Indicative Sources *(Reading lists)*	**Core Material:** • William Stallings and Lawrie Brown (2017), Computer Security: Principles and Practice, Pearson, • ISBN-13: 9781292220611 • Richard Bejtlich (2013), *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, ISBN-10: 1593275099 **Optional** • John Stark (2016), *Hacking: Beginner's Guide to Computer Hacking, Basic Security, Penetration Testing (Hacking, How to Hack, Penetration Testing, Basic security, Computer Hacking)*, CreateSpace Independent Publishing Platform, ISBN-10: 1533258074 • Seymour Bosworth and Michel E. Kabay (2014), *Computer Security Handbook, Set (/)*,John Wiley and Sons, ISBN-10: