Module Descriptor

Title	Enterprise Cybersecurity Management		
Session	2025/26	**Status**	Published
Code	COMP11123	**SCQF Level**	11
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	Computing, Engineering and Physical Sciences		
Module Co-ordinator	Shahriar Al-Ahmed		

Summary of Module

Data and network security have been primary concerns for enterprise in their transition to more efficient and cost effect cloud services. This is due to the fact that the enterprises have no control over the underlying cloud infrastructure (network, computing resources, and storage facility), which is owned, managed, and maintained by a semi-trusted and/or untrusted entities.

With the need of rapid digital transformation in post-COVID world, enterprises are becoming increasingly concerned about their data being persisted, processed, and provisioned outside of their administrative domain; cloud-based storage services are one such example, as these services are typically provisioned by an untrusted cloud service provider.

This module introduces basic enterprise data and network security principles in the context of data transmission and management in untrusted networks. It is intended to cover fundamental data security algorithms and methodologies, laying the groundwork for designing, implementing, and deploying secure and privacy-aware systems for data sharing, collaboration, persistence, and processing within untrusted networks.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module. Universal: Critical Thinker; Ethically-minded; and Research-minded. Work Ready: Problem-Solver; Effective Communicator; and Ambitious. Successful: Autonomous; Resilient; and Driven.

Module Delivery Method	On-Campus[1]	Hybrid[2]	Online[3]	Work -Based Learning[4]
	☒	☐	☐	

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

					□	
Campuses for Module Delivery	□ Ayr □ Dumfries		□ Lanarkshire ☒ London ☒ Paisley		□ Online / Distance Learning □ Other (specify)	
Terms for Module Delivery	Term 1	☒	Term 2	☒	Term 3	☒
Long-thin Delivery over more than one Term	Term 1 – Term 2	□	Term 2 – Term 3	□	Term 3 – Term 1	□

Learning Outcomes	
L1	Demonstrate an extensive knowledge of security and privacy issues related to enterprise data management within untrusted networks and transmission of confidential information over insecure channels
L2	Demonstrate a critical understanding of efficacy of widely used security algorithms, protocols and methodologies for secure and privacy-aware data management in untrusted networks
L3	Develop skills to combine various security and privacy algorithms / protocols to realize privacy-aware solutions for untrusted networks
L4	N/A
L5	N/A

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 11** Students will develop a critical understanding of fundamental enterprise data security concepts, primitives, and principles. They will acquire critical understanding and detail knowledge of security and privacy threats of data transmission over insecure channel. They will obtain critical knowledge of enterprise data security and privacy-aware data management in untrusted networks. They will also carry out critical literature and technical review of enterprise data management in untrusted network as part of their written assignment
Practice: Applied Knowledge and Understanding	**SCQF 11** Students will gain in-depth knowledge about efficacy of conventional systems and their inability to provide higher degree of assurances for enterprise data and network security. They will apply range of specialised skills, techniques and practices to understand limitations of security and privacy methodologies for protecting enterprise data in trusted networks. They will apply knowledge of security and privacy primitives to understand challenges of enterprise data management and collaborative data sharing in untrusted networks
Generic Cognitive skills	**SCQF 11** Students will be able to critically analysis and evaluate efficacy of forefront secure data sharing protocols. They will be able to design and evaluate secure and privacy-aware protocols for collaborative

	enterprise data sharing in untrusted domain. They will be able to identity implications of using conventional security and privacy measures to ensure enterprise data privacy and confidentiality in untrusted networks
Communication, ICT and Numeracy Skills	**SCQF 11** During laboratory and tutorial sessions students will work in groups to discuss on a given enterprise data security and privacy problem. They will develop technical communication skills to share and discuss ideas to solve a particular enterprise data security and privacy scenario which may arise when they are working out of laboratory and lecture room settings. They develop specialised ICT skills to solve, analyse and evaluate enterprise data security and privacy issues
Autonomy, Accountability and Working with Others	**SCQF 11** Each student will generate a comprehensive technical report summarizing the finding for a given relevant topic on computer networks

Prerequisites	Module Code	Module Title
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching

In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.

This module consists of lectures, lab assignments.

Beyond lectures, the goal is to provide knowledge about data transfer through unsecured channels and the management of enterprise data within untrusted networks. Students will study various algorithms, protocols, and procedures for concealing secret information and detecting harmful attempts to tamper with transmitted data through lectures.

Furthermore, students will be introduced to chosen web security issues in order to comprehend vulnerabilities associated with web-based applications.

Labs and tutorial sessions will aid in establishing a thorough comprehension of the information presented in lectures, as well as critical assessment of algorithms and approaches when applied to a specific situation.

This module's material will be given in accordance with the following list of possible topics:

- Concepts of enterprise data security and privacy
- Basic cryptography
- Symmetric encryption
- Message integrity, authentication and split sharing
- Public key cryptography
- Enterprise data security and privacy through trusted third parties
- Authentication protocols
- Real-time communication security

- Selected topics on web security
- Data sharing in untrusted networks

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	Student Learning Hours (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	24
Tutorial / Synchronous Support Activity	8
Laboratory / Practical Demonstration / Workshop	16
Independent Study	152
Please select	
Please select	
TOTAL	200

Indicative Resources
The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Martin, K M. (2017) Everyday Cryptography: Fundamental Principles and Applications, Oxford University Press* Orzach, Y. (2022) Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches, Packt Publishing
(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements
In line with the [Student Attendance and Engagement Procedure](), Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time. **For the purposes of this module, academic engagement equates to the following:** The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity

Supplemental Information

Divisional Programme Board	Computing
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☐ **Yes** ☒ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Business & Applied Computing
Moderator	Raja Majid Ujjan
External Examiner	A Esfahani
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.1

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
During the laboratory sessions, each student will be required to successfully complete the task(s) mentioned in the lab manual (weighted 40%), consequently assessing the achievement of L1
Assessment 2
A formal written report (weighted 60%) will be required from each student summarizing their finding of a given topic and demonstrate their skills to secure enterprise data and network – agreed by the module coordinator, to evaluate L2, L3. This assignment will require the students to do some literature review, identify possible solutions, demonstrate efficacy of proposed solutions, and justify / critics them accordingly
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed.
(ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Clinical/ Fieldwork/ Practical skills assessment/ Debate/ Interview/ Viva voce/ Oral	☒	☐	☐	☐	☐	40	0

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	☐	☒	☒	☐	☐	60	0

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	0 hours

Change Control

What	When	Who
Attendance, EDI and External Examiner updated	22/01/2025	A Adamson