University of the West of Scotland

Module Descriptor

Session: 2023/24

Last modified: 12/04/2023 19:49:04
Status: Published

Title of Module: Enterprise Cybersecurity Management

Code: COMP11123	**SCQF Level: 11** (Scottish Credit and Qualifications Framework)	**Credit Points: 20**	**ECTS: 10** (European Credit Transfer Scheme)
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Graeme A McRobbie		

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

Face-To-Face	Blended	Fully Online	HybridC	HybridO	Work-based Learning

Face-To-Face
Term used to describe the traditional classroom environment where the students and the lecturer meet synchronously in the same room for the whole provision.

Blended
A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered “blended” if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations

Fully Online
Instruction that is solely delivered by web-based or internet-based technologies. This term is used to describe the previously used terms distance learning and e learning.

HybridC
Online with mandatory face-to-face learning on Campus

HybridO
Online with optional face-to-face learning on Campus

Work-based Learning
Learning activities where the main location for the learning experience is in the workplace.

Campus(es) for Module Delivery						
The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit)						
Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
✓				✓		

Term(s) for Module Delivery					
(Provided viable student numbers permit).					
Term 1	✓	Term 2	✓	Term 3	✓

Learning Outcomes: (maximum of 5 statements)

On successful completion of this module the student will be able to:

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

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 Level 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 Level 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 Level 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 Level 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 Level 11. Each student will generate a comprehensive technical report summarizing the finding for a given relevant topic on computer networks

Pre-requisites:	Before undertaking this module the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

* Indicates that module descriptor is not published.

Learning and Teaching

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** (Normally totalling 200 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
	200 Hours Total

****Indicative Resources: (eg. Core text, journals, internet access)**

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)

Engagement Requirements

In line with the Academic Engagement Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on the relevant learning platform, and complete assessments and submit these on time. Please refer to the Academic Engagement Procedure at the following link: Academic engagement procedure

Supplemental Information

Programme Board	
Assessment Results (Pass/Fail)	No
Subject Panel	Applied and Business Computing
Moderator	tbc
External Examiner	tbc
Accreditation Details	pending
Changes/Version Number	1

Assessment: (also refer to Assessment Outcomes Grids below)

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

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

(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 Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Clinical/ Fieldwork/ Practical skills assessment/ Debate/ Interview/ Viva voce/ Oral	✓			40	0

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Report of practical/ field/ clinical work		✓	✓	60	0
			Combined Total For All Components	100%	0 hours

Footnotes
A. Referred to within Assessment Section above
B. Identified in the Learning Outcome Section above

Note(s):
1. More than one assessment method can be used to assess individual learning outcomes.
2. Schools are responsible for determining student contact hours. Please refer to University Policy on contact hours (extract contained within section 10 of the Module Descriptor guidance note).
   This will normally be variable across Schools, dependent on Programmes &/or Professional requirements.

Equality and Diversity

UWS Equality and Diversity Policy

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)