University of the West of Scotland

Module Descriptor

Session: 2023/24

Last modified: 14/04/2023 11:40:39
Status: Published

Title of Module: Network Security Issues

Code: COMP11118	**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

The security of computer networks has been a major concern for the management of information systems used by businesses of all kinds, from start-ups to enterprises. Computer networks are frequently compromised as a result of insufficient security and management measures to detect malicious access privilege escalation, monitor network traffic and services, ensure network confidentiality and privacy, prevent network attacks, and build resilience to modern-day cyber-attacks.

This module discusses network security fundamentals within the context of network and data management for trustworthy and untrusted computer networks.

It is intended to cover key network security approaches, algorithms, and tools, as well as provide hands-on experience in creating and operating secure, privacy-aware, and resilient computer 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 extensive knowledge of the core theories, concepts and principles of secure network design, attacks, and mitigation techniques

L2. Demonstrate a comprehensive understanding of network security frameworks and best practices

L3. Develop skills to analyse and critically evaluate security of networked systems and recommend relevant technical and management improvements or solutions

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 learn comprehensive knowledge of network security. Students are expected to be familiar with the key technologies and techniques and their application in practice
Practice: Applied Knowledge and Understanding	SCQF Level 11. Students will gain in-depth understanding and critical awareness of knowledge of network security, and apply this in planning, implementing, configuration and testing of the security state of the test environment. They will also develop capability to apply a range of specialised research skills and relevant tools and software for their written assignment and lab tasks
Generic Cognitive skills	SCQF Level 11. To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry
Communication, ICT and Numeracy Skills	SCQF Level 11. Working in interacting groups, students will develop communication skills as well as the ability to write technical reports and documentation
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 includes interactive lectures and lab sessions, as well as problem-based learning exercises and corresponding practical workshops. Beyond lectures, the rationale is to impart information linked to computer network administration, data transfer, and network security. Students will study various algorithms, protocols, and strategies for securing computer networks of various sizes and configurations through lectures. Furthermore, students will be taught to specific cybersecurity issues to help them comprehend vulnerabilities in the network generation of computer networks. The lab sessions will aid in the development of an in-depth comprehension of the knowledge presented in the lectures, as well as the critical evaluation 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:
• Common networked system risks and weaknesses
• Network perimeter methods.
• Techniques for network monitoring.
• Cryptographic techniques.
• Protocols and techniques for network authentication.
• Data transfer across a secure network.
• Secure network architecture

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	20
Tutorial/Synchronous Support Activity	4
Laboratory/Practical Demonstration/Workshop	18
Independent Study	158
	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:

Leirvik, R. (2021) Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program, Apress

Diogenes, Y and Ozkaya, E. (2018) Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. 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	Computing
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 network and network services – 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
Laboratory/ Clinical/ Field notebook	✓			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)