University of the West of Scotland

Module Descriptor

Session: 2024/25

Title of Module: Secure Programming			
Code: COMP10068	**SCQF Level: 10 (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:	Paul Keir		

Summary of Module

Security in software begins with an initial design and engineering effort, conscious of classic and contemporary security vulnerabilities; as well as corresponding remedial actions and protocols. In this hands-on module we will first explore the nature of secure programming before introducing a taxonomy of established coding errors, as well as information sources such as the MITRE reference system for Common Vulnerabilities and Exposures (CVE). Conventional programming languages including assembly language, C, C++ and Java, along with related compiler tools, form a foundation for the module, while the benefits of contemporary languages such as Mozilla's Rust and Apple's Swift are also thoroughly analysed. The relevance of strong, static typing; functional programming; advanced type systems; and theorem provers for secure software development will also be introduced.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module: Universal (Analytical, Critical Thinker & Socially Responsible), Work Ready (Digitally Literate, Problem-Solver& Ambitious), and Successful (Incisive, Creative & Autonomous).

Module Delivery Method

Face-To-Face	Blended	Fully Online	HybridC	Hybrid 0	Work-Based Learning
☒	☒	☐	☐	☐	☐

See Guidance Note for details.

If this module is delivered within the BSc (Hons) IT Software Development Programme the 'Blended' module delivery method applies

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) (tick as appropriate)						
Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
☐	☐	☐	☒	☐	☐	Add name

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

Learning Outcomes: (maximum of 5 statements) **These should take cognisance of the SCQF level descriptors and be at the appropriate level for the module.** At the end of this module the student will be able to:	
L1	Demonstrate knowledge that covers and integrates most of the principal areas, features, boundaries, terminology and conventions of cyber security and secure programming.
L2	Critically identify, define, conceptualise and analyse both public and private programmatic security hazards.
L3	Use a range of tools and formal methods to audit and support the development of secure software.
L4	Apply knowledge, skills and understanding of the security features offered by a range of programming languages and libraries.

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 **10** Recognise CVE ID numbers, and prepare a response appropriate to the associated threat level. Comprehend the relationship between a programming language and the underlying computer hardware; the abstract machine.
Practice: Applied Knowledge and Understanding	SCQF Level **10** Apply standard secure coding guidelines to avoid common security loopholes. Demonstrate the utility of tools such as compilers; debuggers; profilers; model checkers; and virtual machines for secure

	programming.	
Generic Cognitive skills	SCQF Level **10** Understand the advantages and limitations of programming within an advanced type system. Appreciate the feature set of libraries for authentication and encryption.	
Communication, ICT and Numeracy Skills	SCQF Level **10** Apply secure software development principles to a range of application domains.	
Autonomy, Accountability and Working with others	SCQF Level Choose an item. Click or tap here to enter text.	
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	
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.	
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	12
Laboratory/Practical Demonstration/Workshop	12
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:

Robert C. Seacord. Secure Coding in C and C++, Second Edition, Addison Wesley, 2013

Steve Klabnik and Carol NicholsThe Rust Programming Language

Jim Blandy and Jason Orendorff. Programming Rust: Fast, Safe Systems Development, O'Reilly Media, 2017

Secure Programming HOWTO - Creating Secure Software by David Wheeler

John Viega and Matt Messier. Secure Programming Cookbook for C and C++, O'Reilly Media, 2003

Brian Chess and Jacob West. Secure Programming with Static Analysis, Addison-Wesley Professional, 2007

SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems (2016 Edition) available online at http://www.cert.org/secure-coding/products-services/secure-coding-download.cfm

The module coordinator will require virtual machine authoring tools, and ITDS assistance to access licensed operating systems materials.

Please ensure the list is kept short and current. Essential resources should be included, broader resources should be kept for module handbooks / Aula VLE.

Resources should be listed in Right Harvard referencing style or agreed professional body deviation and in alphabetical order.

(**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: 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: https://www.uws.ac.uk/media/6588/student-attendance-and-engagement-procedure-september-2023.pdf

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Please ensure any specific requirements are detailed in this section. Module Co-ordinators should consider the accessibility of their module for groups with protected characteristics..
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	Computing
Assessment Results (Pass/Fail)	Yes ☐No ☒
School Assessment Board	Business and Applied Computing
Moderator	Graham Parsonage
External Examiner	Anish Jindal
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	1.10

Assessment: (also refer to Assessment Outcomes Grids below)
This section should make transparent what assessment categories form part of this module (stating what % contributes to the final mark). Maximum of 3 main assessment categories can be identified (which may comprise smaller elements of assessment). **NB: The 30% aggregate regulation (Reg. 3.9) (40% for PG) for each main category must be taken into account. When using PSMD, if all assessments are recorded in the one box, only one assessment grid will show and the 30% (40% at PG) aggregate regulation will not stand. For the aggregate regulation to stand, each component of assessment must be captured in a separate box.** Please provide brief information about the overall approach to assessment that is taken within the module. In order to be flexible with assessment delivery, be brief, but do state assessment type (e.g. written assignment rather than "essay" / presentation, etc) and keep the detail for the module handbook. Click or tap here to enter text.
Assessment 1 - One coursework assignment worth 30% of the overall mark.
Assessment 2 - One coursework assignment worth 40% of the overall mark.
Assessment 3 - One class test worth 30% of the overall mark.
(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.)

Assessment Outcome Grids (See Guidance Note)

Component 1							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Laboratory/ Clinical/ Fieldnote book		X	X	X		30	0

Component 2							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Laboratory/ Clinical/ Fieldnote book		X	X	X		40	0

Component 3							
Assessment Type (Footnote B.)	**Learning Outcome (1)**	**Learning Outcome (2)**	**Learning Outcome (3)**	**Learning Outcome (4)**	**Learning Outcome (5)**	**Weighting (%) of Assessment Element**	**Timetabled Contact Hours**
Class test (practical)	X			X		30	0
Combined Total for All Components						**100%**	**XX hours**