University of the West of Scotland

Module Descriptor

Session:

Title of Module: IoT Security			
Code:	**SCQF Level: 11 (Scottish Credit and Qualifications Framework)**	**Credit Points: 10**	**ECTS: 5 (European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Althaff Mohideen		

Summary of Module

The module provides students with detailed understanding of the IoT systems, architectures, reference models, IoT devices, the protocols (802.15.4, 6LowPAN, Bluetooth, LoRa, ZigBee) used by sensors and actuators, and the applications that allow analysis and control of IoT systems. Provides understanding of IoT implementations ranging from home automation systems to a nation's critical infrastructure, and learning about major attacks against IoT systems and how to secure the IoT systems from cyber threats.

By using reflection techniques and practical work, students will develop a deeper awareness of the security challenges that exist in IoT systems and develop knowledge and skills required to ensure the security of IoT echo systems.

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
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient

- Driven

Module Delivery Method					
Face-To-Face	**Blended**	**Fully Online**	**HybridC**	**Hybrid 0**	**Work-Based Learning**
☐	☒	☐	☐	☐	☐
See Guidance Note for details.					

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	Build an exemplar IoT system.
L2	Use industry-standard models to explain security requirements in IoT systems
L3	Perform threat modelling activities to evaluate communication security vulnerabilities in IoT systems.
L4	Perform threat modelling activities to evaluate application security vulnerabilities in IoT systems.
L5	Click or tap here to enter text.

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 systematic and comprehensive knowledge of IoT 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, comprehensive understanding and critical awareness of knowledge of IoT Securiyt, and apply this in ensuring the security of IoT systems. They will also develop capability to apply a range of standard and specialised research skills, tools/software, development kit and related techniques in response to application requirements 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 report summarising his/her finding for a given scenario.	
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	**Student Learning Hours** (Normally totalling 200 hours):

undertaken to achieve the module learning outcomes are stated below:	(Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	7
Tutorial/Synchronous Support Activity	7
Laboratory/Practical Demonstration/Workshop	14
Independent Study	72
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
	100 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:

Brian Russell, Drew Van Duren. (2018) 2nd Ed. Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem, Packt publishing

Giacomo Veneri, Antonio Capasso. (2018) Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0. Packt publishing
Click or tap here to enter text.

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:

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	
Assessment Results (Pass/Fail)	Yes ☐No ☒
School Assessment Board	
Moderator	
External Examiner	Format: First initial + Surname. No titles. Please only enter if examiner has been approved for this module.
Accreditation Details	e.g. ACCA Click or tap here to enter text.
Changes/Version Number	1.00

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 - Coursework 1 (50%)
Assessment 2 - Coursework 2 (50%)
(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**
	√	√	√			50	

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**
	√	√	√	√		50	

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**
Combined Total for All Components						**100%**	**XX hours**

Change Control:

What	When	Who
Further guidance on aggregate regulation and application when completing template	16/01/2020	H McLean
Updated contact hours	14/09/21	H McLean
Updated Student Attendance and Engagement Procedure	19/10/2023	C Winter
Updated UWS Equality, Diversity and Human Rights Code	19/10/2023	C Winter
Guidance Note 23-24 provided	12/12/23	D Taylor
General housekeeping to text across sections. .	12/12/23	D Taylor

Version Number: MD Template 1 (2023-24)