MODULE SPECIFICATION

Part 1: Information			
Module Title	IoT Systems Security		
Module Code	UFCF8P-15-M	Level	Level 7
For implementation from	2020-21		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Module Type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co-requisites	None		
Module Entry Requirements	None		
PSRB Requirements	None		

Part 2: Description

Educational Aims: This module will teach students fundamental concepts of security of the Internet of Things (IoT) systems, security paradigms employed in IoT, security and privacy issues, and lightweight security solutions.

The students should expect to be able to apply the taught concepts in the development of IoT systems.

Outline Syllabus: This module will cover:
IoT system security architecture
Authentications/authorization
Relevant secure wireless technologies and networking protocols
Security and privacy concepts
Security over resource-limited devices in IoT
Security challenges

Teaching and Learning Methods: The module will consist of a mixture of lectures and labs.

Part 3: Assessment

Summative assessment includes:

Comp A: Two elements, E-Portfolio and Group project with demo.
Part 1: of this will be individual work (A.1), and,
Part A.2 is a group work. This will include group Portofolio that include demo, source code and short technical report.

Comp B: This is a presentation where each group will clearly describe the design of the solution in part A.2. The demo is already in part A.2, this will be about the aspects related to the system design, it conceptual modules.

Normally students from the same group will be awarded the same mark. However individual mark adjustment may be carried out to cater for significant unbalanced contributions.

Formative feedback will be provided to students during the Lab sessions to prepare students for the coursework.

For resit, a scaled down IoT security solution will be used so that it is appropriate for an individual project.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Portfolio - Component A		24 %	Individual E-Portfolio
Group work - Component A		36 %	Group E-Portfolio and Demo
Presentation - Component B	✓	40 %	Group presentation (20 minutes)
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Portfolio - Component A		24 %	Individual E-portfolio
Project - Component A		36 %	Individual mini-project with short demo
Presentation - Component B	✓	40 %	Individual recorded presentation

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will achieve the following learning outcomes:

Module Learning Outcomes	**Reference**
Demonstrate systematic understanding of the security and privacy issues in the Internet of Things such as in resource-constrained environments	MO1
Conceptualise existing security technologies and protocols specific to IoT systems	MO2
Analyse and critically evaluate different light-weight security solutions in the IoT systems	MO3
Design, implement and test a simple security solution for an IoT system	MO4
Communicate technical solutions clearly	MO5

Contact Hours

Independent Study Hours:

	Independent study/self-guided study	114
	Total Independent Study Hours:	114
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	36
	Total Scheduled Learning and Teaching Hours:	36
	Hours to be allocated	150
	Allocated Hours	150
Reading List	*The reading list for this module can be accessed via the following link:* https://uwe.rl.talis.com/modules/ufcf8p-15-m.html	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: Cyber Security [Sep][FT][Frenchay][1yr] MSc 2020-21 Cyber Security [Sep][PT][Frenchay][2yrs] MSc 2019-20