MODULE SPECIFICATION

Part 1: Information			
Module Title	Embedded Systems Security		
Module Code	UFCFJU-30-2	Level	Level 5
For implementation from	2021-22		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	Networking 2020-21, Operating Systems and Architecture 2020-21		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description
Overview: This module aims to provide apprentices with an in-depth appreciation of embedded devices and their security. An embedded system is a combination of processor, memory, I/O and the OS that forms a device. Embedded systems get infrequent or never get software updates. They are very many identical devices installed, often in critical facilities and systems. Because of this the devices must be made secure. Embedded systems have different characteristics, ubiquity and vulnerabilities to desktop and server systems. Comparisons will be made in the module. Delivery will cover modern system architecture, key technologies, and the security implications of implementing these technologies. In addition, essential general low-level malware techniques will be examined. **Educational Aims:** Contributes to underpinning cyber knowledge and extends it into the field of embedded systems.

Outline Syllabus: You will cover:

Architecture of low powered mobile systems

The nature of security in embedded and network systems

Networking technologies

Boot processes, BIOS, file systems and embedded operating systems

interaction between microprocessor software and signals from sensors, actuators, etc

exploitation of external environment or software-hardware interface and mitigations that may be employed

security challenges of embedded systems, for example:
size, power, processor, memory, bandwidth limitations

Internet of Things

low level mechanisms used by current malware

machine level instruction set

reverse engineering techniques

reverse engineering for malware analysis

de-obfuscation of obfuscated code

anti-debugging mechanisms

Teaching and Learning Methods: Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.

Part 3: Assessment

Component A

A 30 minute presentation & Q&A session will allow students not only to demonstrate their technical knowledge of malware threats, engineering and the techniques required for analysis but also allow them to practice their communication skills. The Q&A session gives the students to think on their feet and also gives the chance to fill in any of the gaps that they may have left in their presentation. on malware threats, engineering and the techniques required for analysis

Students for also complete a series of tasks during classroom time. These tasks will form the basis of a workbook which will be presented fro assessment. The tasks will challenge them to develop independent skills in using and securing embedded systems whilst still allowing them plenty of support in what is likely to be a curriculum area that is very new to them.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A	✓	40 %	30 minute presentation and Q&A session.

Practical Skills Assessment - Component B		60 %	Series of classroom-based tasks involving using and securing embedded systems. The tasks will be recorded in a workbook, signed off and submitted for assessment.
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Presentation - Component A	✓	40 %	30 minute presentation and Q&A session.
Practical Skills Assessment - Component B		60 %	Reworked workbook and practical tasks.

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**
Describe and explain the characteristics and complexity of secure, embedded systems.	MO1
Implement software for selected, novel, embedded devices.	MO2
Analyse and evaluate security threats and vulnerabilities with regards to embedded systems and identify how these can be mitigated.	MO3
Construct software to interact with the real world and analyse for security exploits .	MO4
Analyse malware & identify its mechanisms.	MO5

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75
Total Placement Study Hours:	75
Scheduled Learning and Teaching Hours:	
Face-to-face learning	90
Total Scheduled Learning and Teaching Hours:	90

	Hours to be allocated	300
	Allocated Hours	300
Reading List	*The reading list for this module can be accessed via the following link:* https://rl.talis.com/3/uwe/lists/0C83356E-0AFB-0BE8-BFBA-13F7843897E8.html	

Part 5: Contributes Towards
This module contributes towards the following programmes of study: BSc (Hons) Cyber Security Technical Professional (integrated degree) BSc (Hons) 2020-21