Module Specification

Secure Embedded Systems

Version: 2023-24, v2.0, 27 Jul 2023

Contents

Part 1: Information

Module title: Secure Embedded Systems

Module code: UFCFDL-15-2

Level: Level 5

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: Computer and Network Systems 2023-24

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Pre-requisites: students must take one out of UFCFF6-30-1 Programming in C or UFCFGL-30-1 Programming in C++ or UFCF93-30-1 Computer and Network Systems

Features: Not applicable

Educational aims: See Learning Outcomes

Outline syllabus: In this module you will cover the following areas:

History of mobile devices.

Architecture of low powered mobile systems, exemplified by the ARM - Cortex-M3 processor.

The nature of security in embedded and network systems Cross development and cross compilation

Booting embedded systems JTAG - controlling dead or locked systems, recovering data - system initialization, security implications Memory technologies at the device level - Flash, SD

Networking technologies - wired and wireless

Configuring, building and booting embedded OS

File systems for embedded systems on a range of devices

Open source development methodologies. Working in OS communities, responsibilities, professionalism and legal implications.

Power saving features of mobile and embedded systems: Booting, suspending, sleeping and hibernating

Part 3: Teaching and learning methods

Teaching and learning methods: Laboratory exercises will allow the student to gain familiarization with the tools and techniques required for the implementation and verification of safe embedded systems.

Students will be expected to demonstrate self-direction and originality in their

learning which will be facilitated through student directed tutorials.

Scheduled learning in the form of tutorials, demonstrations and practical classes, will comprise 1/3 of the total study time for this module.

The lecture series will be supported by weekly practical sessions in which the students have the opportunity to apply some of the concepts discussed during the lecture series.

The practicals will allow the students to explore and debug mobile devices and/or device simulations using a range of tools.

Independent learning: will constitute the remaining study time with an expectation that approximately 36 hours will be spent on self-directed study, a further 40 hours in support of the coursework and 16 hours in exam preparation.

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

MO1 Understand the characteristics of secure, low-powered mobile and embedded technology

MO2 Analyse and manipulate higher-level software architectures, file systems and memory

MO3 Develop software for mobile and embedded devices for a range of purposes

MO4 Explore booting and system initialization in a range of devices

MO5 Appraise the role of device drivers in mobile embedded systems

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/index.html

Part 4: Assessment

Assessment strategy: Formative assessment is achieved through the demonstration and discussion of their solutions to the graded problems in the worksheets. The sign off sheet will be handed in as evidence of their work.

Students will also be assessed in their effective use and understanding of the tools and technologies that they utilise.

For the referral coursework it is likely that the student will be required to provide evidence of their achievements on the practical worksheets rather than an in person demonstration.

Assessment tasks:

Examination (Online) (First Sit)
Description: Online written Examination (2 hours)
24 hour window
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO4, MO5

Practical Skills Assessment (First Sit)
Description: Signed off and demonstrated practical worksheets
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Examination (Online) (Resit)

Description: Online written Examination (2 hours)

24 hour window

Weighting: 50 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO4, MO5

Practical Skills Assessment (Resit)

Description: Evidence of completed practical worksheets

Weighting: 50 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2022-23

Cyber Security and Digital Forensics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22