Module Specification

Embedded Systems Security

Version: 2023-24, v2.0, 19 Jul 2023

Contents

Module Specification 1

Part 1: Information 2

Part 2: Description 2

Part 3: Teaching and learning methods 4

Part 4: Assessment 5

Part 5: Contributes towards 6

Part 1: Information

Module title: Embedded Systems Security

Module code: UFCFJU-30-2

Level: Level 5

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field:

Module type: Module

Pre-requisites: Networking 2022-23, Operating Systems and Architecture 2022-23

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body 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.

Features: Not applicable

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

Part 3: Teaching and learning methods

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.

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

MO1 Describe and explain the characteristics and complexity of secure, embedded systems.

MO2 Implement software for selected, novel, embedded devices.

MO3 Analyse and evaluate security threats and vulnerabilities with regards to embedded systems and identify how these can be mitigated.

MO4 Construct software to interact with the real world and analyse for security exploits .

MO5 Analyse malware & identify its mechanisms.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/0C83356E-0AFB-0BE8-BFBA-13F7843897E8.html

Part 4: Assessment

Assessment strategy: The following assessment applies at both first and resit.

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 for 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.

Assessment tasks:

Presentation (First Sit)
Description: 30 minute presentation and Q&A session.
Weighting: 40 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO5

Practical Skills Assessment (First Sit)
Description: 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.
Weighting: 60 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Presentation (Resit)
Description: 30 minute presentation and Q&A session.
Weighting: 40 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO5

Practical Skills Assessment (Resit)
Description: 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.
Weighting: 60 %
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 Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl] BSc (Hons) 2022-23