



Module Specification

IoT 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	3
Part 4: Assessment.....	4
Part 5: Contributes towards	5

Part 1: Information

Module title: IoT Systems Security

Module code: UFCF8P-15-M

Level: Level 7

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: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Not applicable

Features: Not applicable

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

Part 3: Teaching and learning methods

Teaching and learning methods: The module will consist of a mixture of lectures and labs.

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

MO1 Demonstrate systematic understanding of the security and privacy issues in the Internet of Things (IoT) such as in resource-constrained environments and wireless networks

MO2 Conceptualise existing security technologies and communication protocols specific to IoT systems

MO3 Analyse and critically evaluate different light-weight security solutions in the IoT systems

MO4 Design, implement and test a simple security solution for an IoT system

MO5 Communicate technical solutions clearly

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](https://uwe.rl.talis.com/modules/ufcf8p-15-m.html) via the following link <https://uwe.rl.talis.com/modules/ufcf8p-15-m.html>

Part 4: Assessment

Assessment strategy: At both first sit and resit, summative assessment students will work in groups to complete a project to design and implement an IoT security system. Typical group size is 3. They will submit design documents, a document explaining their individual contribution in the group, the source code, demo and presentation.

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 if the groups are, of necessity, small.

Assessment tasks:

Project (First Sit)

Description: Group Project (Demo and Presentation).

Weighting: 100 %

Final assessment: Yes

Group work: Yes

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

Project (Resit)

Description: Group Project (Demo and Presentation).

Weighting: 100 %

Final assessment: Yes

Group work: Yes

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

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [GCET] MSc 2023-24

Cyber Security [Frenchay] MSc 2022-23