Module Specification

Cyber Security Futures Emerging Trends and Challenges

Version: 2023-24, v3.0, 27 Jul 2023

Contents

Part 1: Information

Module title: Cyber Security Futures Emerging Trends and Challenges

Module code: UFCFXN-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: Cyber Security Futures Emerging Trends and Challenges will provide students with an opportunity to engage in supported horizon scanning to identify and explore emerging trends in cyber security. It focuses on discussion and critical analysis of cybersecurity research and insights into the latest contributions of industry and academia researchers.

Features: Not applicable

Educational aims: This module aims to train students in applying a well-defined research process in emerging areas of cybersecurity. Students will learn to analyse complicated and empirical research papers to gain insights into the significant literature contributions and gaps. Students of this module can transfer their knowledge and findings of the assessment in completing their project in the module Cyber Security Research Project.

Outline syllabus: The deep analysis of following emerging and impactful cybersecurity research trends is covered in this module.
Fundamental Cybersecurity
IoT Security
Cloud Security
Machine Learning and Cybersecurity
Deep Learning and Cybersecurity
Blockchain Security for IoT and Cloud
Cyber Physical Systems Security
Digital Twins Security
Deepfakes Security

Part 3: Teaching and learning methods

Teaching and learning methods: Teaching and learning are facilitated through a mixture of lecture and seminar sessions.

During the lecture session, the students are introduced to empirical research in emerging areas of cybersecurity, as mentioned in the module syllabus topics. We analyse the research papers to discuss the problem area, literature review, research methodology, proposed contribution and literature gaps. Based on these discussions, students find more papers from well-known digital databases, such as IEEE, ACM, Springer, Science Direct and others, to analyse during the seminars to address research questions to formulate new research contributions with commercialisation significance. Students present their work in the seminars and work with others in groups to critically discuss their findings.

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

MO1 Evaluate and critique the current trends and challenges in cyber security

MO2 Report on evidenced speculation about likely future trends and their impact

MO3 Communicate complex information clearly and effectively

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: The assessment of this module requires the students to write a proposal for a funding competition based on a real call. However, this work intends to evaluate the skills and knowledge students acquired in this module by analysing emerging cybersecurity research trends and challenges during the seminar activities. Students will be given a few research themes and a proposal template. They will be required to select a research topic in one of the research themes to conduct research and write their funding proposal.

The assignment is based on individual work (report) (100%), focusing on producing a research-driven contribution with commercial value in an emerging area of cybersecurity.

In the referral assessment, students can improve their previous submission or choose a new topic to complete the assessment requirements. It will be the same as the main assessment, 100% report.

Assessment tasks:

Report (First Sit)
Description: Report. Max word limit: 2000
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Report (Resit)
Description: Report. Max word limit: 2000
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

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