Module Specification

Computer and Network Systems

Version: 2025-26, v4.0, Approved

Contents

Part 1: Information

Module title: Computer and Network Systems

Module code: UFCF93-30-1

Level: Level 4

For implementation from: 2025-26

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

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: This introductory module provides first-year students with a comprehensive grounding in computer architecture and networking. Students will explore how modern computer systems are structured and operate, including key components such as processors, memory, and data representation. The module also introduces core concepts of operating systems and computer networks, including communication protocols and security principles. Through a combination of theoretical learning and hands-on activities, students will gain the essential skills

needed to analyse, configure, and troubleshoot computing and network environments, laying the groundwork for more advanced study in cybersecurity and related fields.

Features: Not applicable

Educational aims: This module aims to equip students with foundational knowledge and practical skills in computer architecture and networking. It introduces key concepts in operating systems, network protocols, and cybersecurity, preparing students for more advanced study and enabling them to understand, configure, and troubleshoot basic computing and network systems in secure environments.

Outline syllabus: This module introduces the concepts of computer hardware, operating systems, and networking. It covers:

Computer Architecture and Data Representation

Linux Operating Systems for Cyber Security

Computer Hardware

Computer Networking and Protocols: Network Infrastructure, Network addressing, TCP/IP Protocols.

Practical exploration of network scenarios using tools like Wireshark

Implementing Security Mechanisms like Authentication and Basic Encryption Methods.

Part 3: Teaching and learning methods

Teaching and learning methods: Given the module description and learning outcomes provided, here's a suggested delivery method incorporating one hour of self-directed learning and two hours of supervised hands-on practical labs:

Self-Directed Learning :

Students can utilise online resources, textbooks, lecture notes, and multimedia materials to grasp theoretical concepts related to computer architecture, operating systems, networking fundamentals, and cybersecurity principles.

Assign readings, videos, and online tutorials that cover the foundational aspects of computer architecture, data representation, operating systems, networking protocols, and cybersecurity mechanisms.

Encourage students to engage in reflective activities such as summarising key concepts, answering quiz questions, or participating in online discussions to reinforce their understanding.

Supervised Hands-on Practical Labs:

Conduct weekly supervised practical lab sessions where students can apply the theoretical knowledge gained through self-directed learning.

In these sessions, students can work individually or in small groups to experiment with configuring and troubleshooting simple network setups.

Provide hands-on exercises and lab tasks that require students to implement concepts related to computer architecture, operating systems, networking principles, and cybersecurity mechanisms.

Assign lab projects and case studies that simulate real-world scenarios, allowing students to apply problem-solving skills and critical thinking in addressing cybersecurity challenges.

Offer guidance and support from instructors or lab assistants during the lab sessions to help students overcome difficulties and ensure they grasp the practical aspects effectively.

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

MO1 Demonstrate understanding of the fundamental aspects of computer architecture and data representation.

MO2 Demonstrate practical knowledge of operating systems.

MO3 Demonstrate understanding of the fundamental principles of computer networking, communication protocols, and their significance in cybersecurity.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 192 hours

Face-to-face learning = 108 hours

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 module learning outcomes will be assessed through an in-class test and a set of Practical Skill Assessments. The resit strategy will align with the first attempt.

The in-class test will consist of multiple-choice questions, and marked scripts will be returned promptly to students for immediate feedback.
The Practical Skill Assessments will involve four worksheets, with marked scripts also returned quickly for immediate review.

Assessment tasks:

In-class test (First Sit)
Description: Multiple-choice questionnaire (1 hour).
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2

Practical Skills Assessment (First Sit)
Description: Practical Skills Assessment (four worksheets, each containing a set of questions)
Weighting: 50 %
Final assessment: No

Group work: No
Learning outcomes tested: MO3

In-class test (Resit)
Description: Multiple-choice questionnaire (1 hour).
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2

Practical Skills Assessment (Resit)
Description: Practical Skills Assessment (four worksheets, each containing a set of questions)
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2024-25

Computer Security and Forensics {Foundation} [GCET] DipHE 2024-25

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2024-25

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2024-25

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2024-25

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2024-25

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2025-26

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2025-26