Module Specification

Secure Computer Networks

Version: 2025-26, v3.0, Approved

Contents

Part 1: Information

Module title: Secure Computer Networks

Module code: UFCFLC-30-2

Level: Level 5

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: Computer and Network Systems 2025-26

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module provides an in-depth exploration of secure networking principles, practices, and technologies. It combines theoretical insights with practical skills, enabling students to critically analyse and effectively counteract contemporary cybersecurity threats within networked environments.

Features: Not applicable

Educational aims: The module aims to equip students with a comprehensive understanding of network security mechanisms, develop their practical proficiency in implementing and evaluating secure systems, and foster analytical skills necessary for identifying and mitigating complex cybersecurity threats

Outline syllabus: The indicative syllabus is as follows:

Foundations of Security in Networked Systems:

Principles of security: CIA model, Saltzer and Schroeder's design principles, NIST (National Institute of Standards and Technology) security architecture concepts

Threat landscape: adversarial behaviours, attack types (including supply chain attacks), system and network vulnerabilities

Zero Trust Architecture (ZTA): Principles, components, and implications for network design and access control

Cryptography and Secure Protocols:

Symmetric and asymmetric cryptography

Cryptographic primitives and applications: hashes, digital signatures

Transport Layer Security (TLS) and secure communication: protocol overview, certificate validation, key exchange

Authentication, Access Control, and Identity:

Authentication protocols

Challenge-response authentication, multi-factor approaches

Access control models, identity and credential management

Privacy and accountability in networked systems

Network Security Practices:

Network protocol security and vulnerabilities

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Wireless LAN security: Wireless Security mechanisms, common attack vectors

Virtual Private Networks (VPN), and tunnelling protocols

Secure System Administration:

Securing Linux environments: services, permissions, system hardening
Containerised and virtualised environments for secure configuration
Auditing, logging, patching, and updates

Traffic Analysis and Network Monitoring:
Packet capture and inspection
Analysing normal vs anomalous behaviour
Threat detection and interpretation of indicators of compromise

Applied Security Investigation:
Penetration testing concepts: reconnaissance, scanning, exploitation, clean-up
Secure configuration validation and impact analysis

Part 3: Teaching and learning methods

Teaching and learning methods: The module is delivered through a series of lectures and associated practical sessions.

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

MO1 Demonstrate critical understanding of core network and system security mechanisms, including cryptographic protocols, secure communication standards, and authentication models.

MO2 Implement and conduct practical investigations to configure, monitor, and analyse secure networked systems using appropriate tools, and interpret findings with professional rigour.

MO3 Analyse evolving security threats and apply technical and conceptual knowledge to propose, justify, and evaluate appropriate defences in line with contemporary practice.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 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/modules/ufcflc-30-2.html

Part 4: Assessment

Assessment strategy: The module is assessed through two practical tasks that develop and test students' ability to implement, demonstrate, and evaluate secure networked systems in response to real-world security challenges. Both tasks are designed to promote the development of professional skills through hands-on investigation.

Task 1: Practical Skills Demonstration (Pass/Fail)

Students complete a practical skills assessment that requires them to demonstrate and explain the application of fundamental tools and techniques introduced in the early part of the module. This may include activities such as secure system configuration, traffic analysis, or the application of encryption or authentication protocols.

Purpose: To verify that students can competently execute and communicate foundational security operations using standard tools and practices

Task 2: Applied Security Investigation (100%)

Students are required to design and implement a technical security scenario that simulates a cyber-attack chain within a controlled environment. The scenario must demonstrate adversarial thinking and the application of offensive security techniques (e.g., automation, scripting, or protocol manipulation). Students must detail the design, implementation, execution, and mitigation of the attack, supported by

accompanying technical documentation (e.g., scripts, payloads).

The work should be clearly contextualised, mapped to recognised frameworks (for example MITRE ATT&CK) and include an analysis and justification of defensive measures relevant to the specific tactics and techniques used.

Formative Assessment Opportunities:
Students will have regular formative opportunities through practical workshops, receiving ongoing feedback on their technical skills, investigative strategies, and security analyses to prepare effectively for summative assessments.

Resit Information:
Resit assessments will follow the same format and requirements as the main assessment tasks, ensuring consistency and fairness in evaluation.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: Two practical lab exercises (pass/fail)
Weighting: 0 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Practical Skills Assessment (First Sit)
Description: Implementation of cyber attack.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3

Practical Skills Assessment (Resit)
Description: Two practical lab exercises (pass/fail)
Weighting: 0 %

Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Practical Skills Assessment (Resit)
Description: Implementation of cyber attack.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2024-25

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

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

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

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2024-25

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2023-24

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2023-24

Computer Security and Forensics {Foundation} [GCET] DipHE 2023-24