Module Specification

Computer and Network Security

Version: 2026-27, v2.0, Approved

Contents

Part 1: Information

Module title: Computer and Network Security

Module code: UFCFVN-30-M

Level: Level 7

For implementation from: 2026-27

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 module covers security concepts, threats, mechanisms and services related to Computer and Network Security using practical examples combined with theoretical background.

Features: Not applicable

Educational aims: This module aims to provide students with an advanced and comprehensive understanding of computer networks and their security within the context of contemporary cyber threats. Building on a solid foundation of core networking and security principles, the module is designed to develop both theoretical knowledge and practical skills essential for addressing the challenges faced by modern networked systems.

Students will critically engage with fundamental security concepts, including confidentiality, integrity, availability, authentication, and non-repudiation, as well as a range of threat models and mitigation strategies. The curriculum integrates lectures, seminars, and hands-on practical sessions, ensuring the application of theoretical concepts to real-world scenarios. Case studies of the latest security threats and attacks are used to contextualise learning and highlight the evolving nature of cyber risks.

A distinctive feature of the module is its emphasis on experiential learning. Students will investigate and simulate recent cyber attacks—such as Distributed Denial of Service (DDoS), ransomware, and advanced persistent threats—using industry-standard tools and platforms. This practical approach enables students to understand attacker methodologies, evaluate defensive measures, and develop effective response strategies.

The module also explores emerging technologies, encouraging students to assess their impact on network security. By the end of the module, students will be able to design secure network architectures, identify and respond to sophisticated threats, and critically evaluate security solutions in real-world contexts.

This module prepares students for professional roles in cyber security, network administration, and threat analysis, equipping them with the skills and adaptability required to succeed in a rapidly changing digital landscape.

Outline syllabus: The module topics are likely to include, but are not limited to:

Foundational principles: Definitions and objectives of cyber security, Saltzer and Schroeder's design principles, National Institute of Standards and Technology (NIST) Principles, Security architecture and lifecycle.

Attacks and defences: Malware and Attack Technologies, Adversarial Behaviours, Honeypots and Honeynets, Cyber threat intelligence, Situational awareness.

Cryptography algorithms, Symmetric Cryptography, Public Key Cryptography, Secret sharing.

Authorization, Authentication, Accountability: Access Control, Identity Management, Federated Access Control, Privacy and Accountability.

Software and Platform Security: Software Security; Categories and prevention of vulnerabilities, Mitigation and detection of vulnerabilities, Secure Software Lifecycle, Web and Mobile Security, Network Security; Intrusion Detection, Intrusion Prevention, Network protocol security and vulnerabilities, Wireless Security, Cloud security and security design principles.

Penetration testing: Reconnaissance, Fingerprinting, Attack, Exploit, Clean Up.

Part 3: Teaching and learning methods

Teaching and learning methods: In this module, the learning experience is designed to be dynamic, interactive, and closely aligned with the demands of the cyber security profession. Students will benefit from a blend of teaching and learning methods that combine theoretical foundations with practical, real-world application.

Lectures provide a structured overview of key concepts, emerging threats, and the latest developments in computer networks and security. These are complemented by practical's, where students are encouraged to discuss, debate, and critically analyse contemporary issues and case studies. This approach fosters deeper understanding and helps develop the analytical skills required for advanced study and professional practice.

In general, the module will take a practical approach, offering weekly opportunities to implement aspects of the topics discussed. Students will be expected to develop a portfolio of network security case studies related to the practical lab sessions, alongside one larger research piece focusing on a real-world security incident. These activities are designed to reinforce learning and demonstrate an ability to apply theory to practice.

Collaborative learning is also emphasised, with group projects and peer discussions providing opportunities to share insights and learn from diverse perspectives. Students will be encouraged to reflect on their learning, identify areas for further development, and engage in independent research.

Assessment methods include practical assignments, case study analyses, presentations, and written reports, allowing students to demonstrate knowledge, critical thinking, and technical skills across multiple formats.

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

MO1 Demonstrate a critical understanding of the advanced mechanisms employed to ensure network security.

MO2 Develop a comprehensive and integrated understanding of pivotal topics at the forefront of this field, including recent advancements and unresolved issues.

MO3 Acquire sophisticated practical and analytical skills to remain current with future developments in networking and computing.

MO4 Conduct practical work to investigate techniques covered in this module and provide an in-depth analysis of the findings.

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/ufcfvn-30-m.html

Part 4: Assessment

Assessment strategy: This module's assessment strategy is designed to enable students to achieve the stated learning outcomes through a balanced combination of theoretical analysis and practical application. It reflects the principles of the university's Academic Regulations and Enhancement Framework, ensuring fairness, rigour, and relevance to professional practice.

Assessment is structured around two individual portfolio submissions, each worth 50% of the overall module mark. Each portfolio incorporates two assessed skill test labs to evaluate hands-on proficiency and ensure alignment with the module and programmatic learning outcomes.

Portfolio 1 – Critical and Theoretical Analysis
This portfolio assesses the ability to critically engage with advanced network security mechanisms and demonstrate a comprehensive understanding of current and emerging issues. It includes written analyses of key security protocols and technologies, critical reviews of recent developments and unresolved challenges, and assessed lab-based skill tests to apply theoretical concepts in practice.

Portfolio 2 – Practical Application and Investigation
This portfolio evaluates the ability to apply advanced practical and analytical skills through a portfolio of case studies based on two assessed labs and an in-depth investigation of a real-world security incident. Assessed lab-based skill tests are included to demonstrate technical competence in realistic environments.

Both portfolios are individual submissions, designed to promote independent learning. Tasks are scenario-based and personalised. The inclusion of reflective commentary and practical artefacts further supports originality and integrity. These will also include video and written report elements.

Formative assessment is embedded throughout the module via feedback during weekly lab sessions, and tutor-led discussions of tasks. These opportunities allow students to refine their understanding and improve performance ahead of final submission.

This strategy ensures that students are assessed holistically, developing both academic insight and practical capability in line with the expectations of a Master's-level cyber security programme.

The resit structure is the same as the first sit, but there is limited support in terms of formative feedback and lab sessions for resit.

Assessment tasks:

Portfolio (First Sit)
Description: Portfolio 1 of Network Security projects (5-10 hours)
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Portfolio (First Sit)
Description: Portfolio 2 of Network Security projects (5-10 hours)
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO4

Portfolio (Resit)
Description: Portfolio 1 of Network Security projects (5-10 hours)
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Portfolio (Resit)

Description: Portfolio 1 of Network Security projects (5-10 hours)

Weighting: 50 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Frenchay] MSc 2026-27

Cyber Security [Frenchay] MSc 2026-27

Cyber Security [GCET] MSc 2026-27

Cyber Security {with International Pre-Masters} [UWEBIC] MSc 2026-27