Module Specification

Computer and Network Security

Version: 2021-22, v3.0, 12 Jul 2021

Contents

Part 1: Information

Module title: Computer and Network Security

Module code: UFCFVN-30-M

Level: Level 7

For implementation from: 2021-22

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Delivery locations: Frenchay Campus

Field: Computer Science and Creative Technologies

Module type: Standard

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: In its initial stages, this module reviews and consolidates knowledge of fundamental security concepts, threats, mechanisms, and services. On the basis of an established knowledge base, more advanced topics are presented, explored and discussed through a combination of lectures and practical sessions. Latest security threat and attack case studies will provide context to the teaching topics.

Outline syllabus: The module will cover the following topics:

Foundational principles: Definitions and objectives of cyber security, Saltzer and Schroeder's design principles, NIST Principles, Security architecture and lifecycle.

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

Cryptography: AES, RSA, DES, PKCS, DSA, Kerberos, TLS, 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 LAN 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 general, the module will take a practical approach, offering the students weekly opportunities to implement aspects of the topics discussed. In addition, students will be expected to develop a portfolio of network security case studies related to the practical lab sessions and one larger research piece focusing on a real-world case study of a security related incident.

Module Learning outcomes:

MO1 Demonstrate critical understanding of the mechanisms used to maintain network security

MO2 Have a deep and integrated understanding of selected key topics at the forefront of this field, including recent developments and outstanding issues

MO3 Have practical and analytical skills to keep abreast of future developments in networking and computer

MO4 Be able to undertake practical work that explores techniques covered in this module and provide deep analysis on their findings

MO5 Ability to undertake and report on a detailed practical investigation at a professional standard

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Laboratory work = 48 hours

Total = 300

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: The emphasis in this module is in ensuring that students are able to undertake the practical implementation of aspects of network security. The summative assessment, therefore, requires them to work with case studies, to analyse the security deficiencies and to use their practical skills to improve on those.

The students undertake a range of tasks that are presented as a portfolio. This task is split into two to give an opportunity for summative as well as formative feedback during the module. The students develop a portfolio of network security case studies and submit a report on each (which may include code) which analyses the security aspects of their implementation. Each report will also contain an additional element of a research based task to further explore the area.

Formative assessment will be provided as oral feedback throughout the laboratory sessions particularly with respect to the regular practical lab exercise.

The resit is the same as the first sit.

Assessment components:

Portfolio - Component A (First Sit)
Description: Portfolio 1 of Network Security projects
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Portfolio - Component A (First Sit)
Description: Portfolio 2 of Network security projects
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Portfolio - Component A (Resit)
Description: Portfolio 1 of Network Security projects
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Portfolio - Component A (Resit)

Description: Portfolio 2 of Network Security projects

Weighting: 50 %

Final assessment: Yes

Group work: No

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

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Sep][PT][Frenchay][2yrs] MSc 2021-22

Cyber Security [Sep][FT][Frenchay][1yr] MSc 2021-22