Module Specification

Secure Computer Networks

Version: 2023-24, v2.0, 16 Jan 2023

Contents

Part 1: Information

Module title: Secure Computer Networks

Module code: UFCFLC-30-2

Level: Level 5

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

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: Computer and Network Systems 2023-24

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: See Learning Outcomes

Outline syllabus: Computer network architectures and models Layered models, peer protocols, the ISO OSI model

Protocol Specification and Design Specification techniques - FSM, layered protocols, error correction

Connection vs connectionless protocols

Medium Access Control Protocols MAC techniques

Subnetworks and Internetworks network layer design, routing and switching, addressing and naming network topology

Transport Services TLIs

Network & Distributed Systems Management Security issues, fault, monitoring and accounting issues.

TCP/IP protocols IP layer, ICMP, ARP TCP socket programming Applications IPV4 and IPng Administering a TCP IP network

System Administration Specifying and installing an OS and network Initialise the system for user and applications Install devices, software packages and communication links

Making the system secure, investigation of security strategies Instigation of system maintenance - backup, user control Document system and system modifications

Security, trust, policy. Threats and protection mechanisms. Systems trusted to deliver confidentiality and integrity; trust; security as policy; protection as a mechanism against a threat; security life cycle; layering and distribution of security mechanisms.

Threats: Interception; interruption; modification; fabrication; types of attack; eavesdropping; masquerading; message tampering; replaying; denial of service.

Protection Mechanisms: Encryption (key cryptography): public (RSA); secret (DES, 3

DES); cryptographic hash functions (SHA1, MD5); stream/block ciphers.

Authentication Protocols: Challenge response; secret key; key distribution centre (Kerberos); Needham- Schroeder protocol; public key. Public Key Management: Certificates (X509); Certification Authorities and PKI; PKI Issues; .NET Passport.

Digital Signatures (Message Integrity): Authorization and access control; access control lists; capabilities; protection domains; firewalls; auditing.

Secure Internet Protocols: Secure Socket Layer SSL (RFC 2246); GSSAPI; DNSSEC; IPSec.

Security and Mobility: WLAN security; GSM/GPRS/UMTS security

Part 3: Teaching and learning methods

Teaching and learning methods: See Assessment

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

MO1 Demonstrate an understanding of a range of protocols employed at various network layers

MO2 Appreciate the significance of end-to-end security in network communication

MO3 Communicate the nature and potential of threats to the security of computer networks, systems and operating systems

MO4 Discuss the relative merits of different solutions to these threats for a given system, business or application

MO5 Analyse a typical business/application for security threats, using appropriate models and leading to proposed solutions

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

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

Part 4: Assessment

Assessment strategy: The module is assessed by two tasks which enable students to achieve an understanding of the underlying principles of security protocols and system vulnerabilities

Task 1 : is a series of laboratory based exercises designed to introduce students to concepts and consolidate understanding through practice.
Task 2: The knowledge and skills gained from task 1 feed directly into task 2 which is an extended problem which involves a systematic investigation into the threats to the security of computer networks, systems or operating systems

Both tasks cover the same module learning outcomes and the resit assessment strategy repeats the tasks set out in the 1st sit.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: Set of regular practical lab exercises (pass/fail)
Weighting:
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Written Assignment (First Sit)

Description: A practical piece of work involving programme code

Weighting: 100 %

Final assessment: No

Group work: No

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

Practical Skills Assessment (Resit)

Description: Laboratory workbook exercises (pass/fail)

Weighting:

Final assessment: No

Group work: No

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

Written Assignment (Resit)

Description: A practical piece of work involving programme code

Weighting: 100 %

Final assessment: No

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 and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

Forensic Computing and Security {Dual} [Mar][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Forensic Computing and Security {Dual} [Aug][FT][Taylors][3yrs] - Not Running BSc (Hons) 2022-23

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2022-23

Cyber Security and Digital Forensics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Feb][FT][GCET][4yrs] BSc (Hons) 2021-22

Computer Security and Forensics {Foundation} [Oct][FT][GCET][4yrs] BSc (Hons) 2021-22