STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Information

Module Title	Secure Computer Networks		
Module Code	UFCFLC-30-2	Level	Level 5
For implementation from	2018-19		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Contributes towards			
Module type:	Standard		
Pre-requisites	Computer and Network Systems 2018-19		
Excluded Combinations	Advanced Systems Administration (10 Credits) 2017-18		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

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

Teaching and Learning Methods: See Assessment

Part 3: Assessment

The module is assessed by 2 1.5-hour exams, which will be taken in January (multiple choice) and at the end of the course – written exam. In addition, students will complete a piece of coursework. The coursework is designed to test the students' capacity to implement the ideas presented in the lectures and to consolidate the practical/tutorial sessions. Students should expect to spend approximately 40 hours completing the coursework.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Practical Skills Assessment - Component B		60 %	A practical piece of work, involving programme code
Practical Skills Assessment - Component B		15 %	Set of regular practical lab exercises
Examination - Component A	✓	15 %	Examination 2 (1.5 hour) – June
Examination - Component A		10 %	Examination 1 (1.5 hour) – January

Resit Components	**Final Assessment**	**Element weighting**	**Description**
Practical Skills Assessment - Component B		75 %	A practical piece of work involving programme code
Examination - Component A	✓	25 %	Examination (2 hours)

Part 4: Teaching and Learning Methods	
Learning Outcomes	On successful completion of this module students will be able to:

	Module 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

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	228
Total Independent Study Hours:	228
Scheduled Learning and Teaching Hours:	
Face-to-face learning	72
Total Scheduled Learning and Teaching Hours:	72
Hours to be allocated	300
Allocated Hours	300

Reading List	*The reading list for this module can be accessed via the following link:* https://uwe.rl.talis.com/modules/ufcflc-30-2.html