STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Information			
Module Title	Computer and Network Security		
Module Code	UFCFVN-30-M	Level	Level 7
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	Cyber Security [Sep][FT][Frenchay][1yr] MSc 2018-19 Cyber Security [Sep][PT][Frenchay][2yrs] MSc 2018-19		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

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 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:

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

Protection Mechanisms: Encryption (key cryptography): public (e.g. RSA-OAEP); secret (e.g. AES); cryptographic hash functions (e.g. SHA3).

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

Digital Signatures (Message Integrity): Authorization and access control; access control lists; capabilities; protection domains; firewalls; auditing, password management, threats, and mitigation.

Secure Internet Protocols, for example, TLS, DNSSEC, Secure BGP protocol. Secure Socket Layer SSL (RFC 2246); GSSAPI; DNSSEC; IPSec.

Security and Mobility: WLAN security; agents and mobile code; protecting an agent (selective revealing); sandbox approach, security libraries.

Systems trusted to deliver confidentiality and integrity; trust; security as policy; protection as a mechanism against a threat; the security lifecycle; layering and distribution of security mechanisms.

Cloud security, security design principles.

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

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 undertake a more substantial piece of practical work and this work will form the basis of their assessment.

Contact Hours:

Activity:
Contact: 48 hours
Assimilation and skill development: 148 hours
Undertaking coursework: 40 hours
Research and demonstration of practical labs: 64 hours
Total: 300 hours

The table below indicates as a percentage the total assessment of the module which constitutes a;
A: A demonstration of a case study based security task
B: The code and documentation associated with the task above.

Part 3: Assessment

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 a case study, to analyze the security deficiencies and to use their practical skills to improve on those.

In the controlled condition element of assessment (component A) students will be required to demonstrate their work. During the demonstration, they will be expected to discuss the security-related choices that they made and the rationale for those choices.

Component B requires the students to submit the code associated with their project together with a report which analyses the security aspects of their implementation. Indicative topics for analysis are efficiency, effectiveness, significance relative to common attack vectors, the extent to which security vulnerabilities remain etc.

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

Total Assessment:

A: Demonstration of a case study based security task: 25% B: The code and documentation associated with the task above: 75% Total: 100%			
First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Project - Component B		75 %	Network security project requiring implementation and documentation
Practical Skills Assessment - Component A	✓	25 %	Project demonstration
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Project - Component B		75 %	Network security project requiring implementation and documentation
Practical Skills Assessment - Component A	✓	25 %	Project demonstration

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will be able to:

	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	Be able to undertake an investigation into areas covered by this module and report on their findings

Contact Hours

Contact Hours	
Independent Study Hours:	
Independent study/self-guided study	200
Total Independent Study Hours:	200
Scheduled Learning and Teaching Hours:	
Face-to-face learning	72

	Laboratory work	28
	Total Scheduled Learning and Teaching Hours:	100
	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/index.html	