MODULE DESCRIPTOR

Module Title

Internet Security

Reference	ENM174	Version	6
Created	August 2021	SCQF Level	SCQF 11
Approved	March 2004	SCQF Points	15
Amended	August 2021	ECTS Points	7.5

Aims of Module

To provide the student with the ability to understand and manage the security and client-server (e.g. web-server) aspects of computer networks with Internet access.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1 Evaluate the security implications of computer networks and develop a security policy to protect systems and data.

2 Define and evaluate systems to protect network users from computer viruses and hostile applications.

3 Identify and evaluate suitable file and data encryption mechanisms to prevent eavesdropping and protect privacy.

4 Define and evaluate counter measures to combat against unauthorised network access.

5 Implement systems to protect network users from computer viruses, hostile applications and combat against unauthorised network access.

Indicative Module Content

Security policy objectives: availability, integrity, privacy, authenticity; assessing exposure, countermeasures. Threat reduction analysis. Methods of attack: Eavesdropping, spoofing, Trojan horses, viruses, denial of service. Protection mechanisms: DES and Public Key encryption, Secure Socket layer (SSL) for web transactions, digital signatures. Firewall configuration and the de-militarised zone. Virtual Private Networks (VPN). Access Control Lists.

Module Delivery

The module is taught using a structured programme of lectures, tutorials, practical exercises and student-centred learning.

Indicative Student Workload	Full Time	Part Time
Contact Hours	38	38
Non-Contact Hours	112	112
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	30%	Outcomes Assessed:	5
Description:	Practical exercises implementing security measures on a network.				

Component 2

Type:	Examination	Weighting:	70%	Outcomes Assessed:	1, 2, 3, 4
Description:	Closed book examination.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The module has 2 components and an overall grade D is required to pass the module. The component weighting is as follows: C1 is worth 30% and C2 is worth 70%.

		Coursework:					
		A	**B**	**C**	**D**	**E**	**F**	**NS**
Examination:	**A**	A	A	B	B	B	E	
	B	B	B	B	C	C	E	
	C	B	C	C	C	D	E	
	D	C	C	D	D	D	E	
	E	D	D	D	E	E	E	
	F	E	E	E	E	F	F	
	NS	Non-submission of work by published deadline or non-attendance for examination						

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1 STALLINGS, W., 2006. Cryptography and Network Security. New Jersey:Prentice Hall.

2 SCHNEIER, B., 2004. Secret and Lies, New York:John Wiley.

3 ANDERSON, R., 2008. Security Engineering. New York:John Wiley.