Module Title
Internet Security

Keywords
Network Security, Encryption, Privacy, Digital Signatures, Client-server, Counter-measures

Reference	ENM174
SCQF Level	SCQF 11
SCQF Points	15
ECTS Points	7.5
Created	May 2002
Approved	March 2004
Amended	August 2011
Version No.	4

This Version is No Longer Current

The latest version of this module is available here

Prerequisites for Module

None.

Corequisite Modules

None.

Precluded Modules

None.

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

Indicative Student Workload

Contact Hours	Full Time	Part Time	Distance Learning
Assessments	14	14	14
Lectures	12	12	0
Tutorials/Seminars	12	12	0
Directed Study			
	37	37	37
Private Study			
	75	75	75
Self-directed study of on-line materials	0	0	24

Mode of Delivery

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

Assessment Plan

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. Implement systems to protect network users from computer viruses and hostile applications.
3. Identify suitable file and data encryption mechanisms to prevent eavesdropping and protect privacy.
4. Define and implement counter measures to 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.

	Learning Outcomes Assessed
Component 1	2,3,4
Component 2	1,2,3,4

Component 2 is a closed book exam. (70% weighting).

Component 1 involves reporting on practical exercises implementing security measures on a network. (30% weighting).

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.

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.