MODULE DESCRIPTOR

MODULE TITLE	Computer Security		
MODULE CODE	CO2508 (L5)	CREDIT VALUE	20 / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE AIMS

Organisations and individuals depend on the security of their computer systems to protect those systems and the data that they store, process, and communicate. The data might be, for example: personal and financial details; medical databases; research databases; commercial or military secrets and designs; commercial orders; and so on. Computers might control sophisticated (and perhaps dangerous) hardware. Damage or loss through accident or malicious attack can have serious implications for those affected and can threaten the existence of organisations. Society has become so heavily dependent on computers and networks to support its functioning that computer security is a fundamental human concern.

The personal and economic effects of loss are greater than ever. Moreover, systems are now potentially vulnerable to a wider range of threats, particularly because of the widespread access to the Internet.

To be effective, security measures must be designed into the system and integrated, covering hardware, software, physical and human aspects. Those responsible for the design and implementation of computer security systems require both technical knowledge and an appreciation of the human aspects. They must ensure that the measures are appropriate, cost-effective, and put into action.

The threats and countermeasures are constantly changing. This module examines the technology in sufficient depth to allow the student to adapt to future challenges. It addresses human aspects at a personal and policy level.

Aims

1. To examine a range of vulnerabilities and attacks on computer systems and networks.
2. To instil a vigilant attitude towards potential system weaknesses.
3. To develop an understanding of methods for protecting communication and computer systems.
4. To encourage a systematic approach to computer security.
5. To integrate the students’ skills by tackling the complex problem of system security.

MODULE CONTENT

Since security threats are changing as the cyber-criminals constantly search for new opportunities and better ways to exploit weaknesses in system defences, countermeasures must also develop to match these. Consequently, the content of the course must adapt to remain relevant however, the general principles tend to hold firm and these will form the backbone of the course.

Indicative content is outlined below:

Key Concepts of Protection

Security policies
Such as Acceptable Use Statement, ethical behaviour standards, and procedures including risk analysis.

Access Controls
Identification and authentication procedures, password security, biometric systems and the intrinsic security of operating systems along with access control lists.

Cryptography
Symmetric encryption. Asymmetric encryption. Key distribution. Digital certificates. Digital signatures. Hash functions.

General Security Measures
Intrusion Detection systems, Firewalls, DMZ, Antivirus screening, Intrusion Detection Systems and Observing usage, for example Log files.

Key Elements of Attack

Reconnaissance
Finding information about computer systems involves a wide range of activities from accessing general information: Public information and whois databases to employing Port scanning, Vulnerability scanning and Network Mapping tools. The legitimate and illegitimate uses of security software.

Spoofing
IP spoofing, Mail spoofing, Website spoofing. Source routing. Trust relationships. Man-in-the-middle attacks. Cookies; tracking. Social engineering.

Coding Security
Buffer overflows; stack, heap overflows; stack canary; etc.

Threat Landscape
Overview of malware. Case studies of security breaches and attacks.

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Discuss potential threats to computer systems and networks.
2. Propose and justify suitable security measures for a networked computer system.
3. Explain the role of cryptographic techniques.
4. Evaluate tools and techniques for system security.

TEACHING METHODS

The module examines a useful range of the fundamental aspects of computer security. Lectures provide the formal taught content, while the practical / tutorial sessions supplement and support the lectures using a series of mini-assignments that allow a discovery approach to learning. Case studies of security breaches and attacks are also discussed.

Students are directed to supplementary reading material that elaborates on the topics covered, at the appropriate level for this module.

The subject material and the software employed have the potential to be used legitimately and illegitimately. Students are therefore required to create for themselves, in a democratic exercise, an “Acceptable Use Statement” for the ethical operation of the module, with appropriate penalties for its contravention. All students must sign this statement before the practical / tutorial sessions can begin.

The summative assessment is designed to test the students’ comprehension and application of the concepts taught or discovered in a written examination and their practical skills in the use of security tools and techniques in a coursework assignment.

.

ASSESSMENT METHODS

This module is assessed through a report (50%) and an examination (50%).