MODULE **DESCRIPTOR**

MODULE TITLE	DIGITAL SECURITY		
MODULE CODE	CO4509 (L7)	**CREDIT VALUE**	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

Businesses depend on IT systems and the valuable data they store, manipulate and communicate. Since data includes personal and financial information, commercial secrets, designs, orders and plans, loss through accident or malicious attack can threaten the very existence of an organisation.

Increasingly, digital networks are essential to support the daily operations of a business. Not only are the economic effects of loss greater than ever, systems are now more vulnerable to a wider variety of threats and especially to risks posed by the greater access to systems provided by the Internet.

To be effective, security measures must cover hardware, software, physical and human issues and be designed into the system. Those responsible for the design and implementation of the security system require significant technical skills and an appreciation of human issues. They must ensure that the measures are cost-effective and appropriate, 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 issues at a personal and policy level.

This module 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 enable students to evaluate methods for protecting communication and computer systems
4. To encourage a systematic approach to computer security
5. To develop research and analysis skills

MODULE **CONTENT**

Indicative syllabus content:

Threats and Counter-Measures
A detailed investigation of various attacks and countermeasures, for example, examining virus-writing techniques at a program and system level for Windows and UNIX operating systems. Email attacks and security through encryption.
Viruses, including macro and script viruses, hoax pseudo-viruses, Trojans, Worms, Denial of Service Attacks, Buffer Overflow, etc.
Evaluation of approaches to Virus prevention and detection: techniques, software, and system policies.
Encryption
Techniques and applications for public and private key cryptography, public and private keys, key distribution, attacks, steganography. Cryptographic algorithms and relevant mathematics. Quantum cryptography.
Introduction to Security in Networks
Port security, port scanners, Packet Filtering, Firewalls, de-militarised zones, System probing software, spoofing attacks.
Operating System Security
Passwords and access rights, obtaining administrator/root privileges. Evaluation of security models, including Windows and Unix, and security standards
Data Security
Importance of data security: commercial issues, legal issues – e.g. Data Protection Act, Regulation of Investigative Powers
Risk Analysis: threat identification, evaluation, management
Specific security measures: Physical Security including biometrics, Personnel Security, Document Security, Hardware security, Processes e.g. backup.

System Security Policies

Guidelines on policy development, data protection policy, security policy, business continuity planning, system access control, physical and environmental security, compliance, personnel and organisational security, human problems of excessive security. Security Standards e.g. ISO 17799.

INTENDED **LEARNING OUTCOMES**

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

1. Analyse potential threats to computer systems and networks and evaluate countermeasures.
2. Propose and justify suitable security for a networked computer system.
3. Use and critically evaluate tools and techniques for system security.
4. Critically evaluate security policies and techniques.
5. Research and report on a security-related topic, using appropriate literature.

TEACHING METHODS

A themed approach will be used to avoid the module becoming a cookbook of disjoint techniques.

Practical classes will examine software techniques used by viruses, provide experience of security facilities and tools under the Unix and Windows operating systems and demonstrate the use of hardware and software techniques for securing communications systems. This will contribute to a practical assignment which is to assess the security and then secure a system.

During tutorials, the class will examine case scenarios and evaluate potential approaches based on techniques introduced and explained in lectures. Lectures will also outline topics for research; and direct reading to selected references. Students will investigate and report on techniques and threats using appropriate literature.

Although aspects of this subject can be very technical, there are many interesting and relevant articles appropriate for this module. They will feed into both assignments. One assignment will be a literature review related to a current security topic, for instance cloud, Heartbleed or WannaCry. This will assess the student's ability to find and integrate relevant material.

The other assignment will be the creation of a portfolio based around practical exercises, including a write-up of results and additional investigation.

If used maliciously, the capabilities developed in this module have potential for harm. Staff will stress the students' ethical responsibilities and students will sign to confirm their adherence to professional guidelines (BCS code of practice, Computer Misuse Act).

ASSESSMENT METHODS

This module is assessed through an examination and a report.