Module Code: CIS 2390
Module Title: OPERATING SYSTEMS AND NETWORK SECURITY

Scheme: Undergraduate Computing
Module rating: Intermediate, 20 credits
Delivery Method: **Lectures**: 24 hrs
Tutorials/Practicals: 24 hrs
Directed Unsupervised Activity: 152 hrs
School(s) involved: Computing and Engineering
Module author(s): Roger England and Peter Hood
Prerequisites: Hardware and Networks or Hardware and networks for the Secure Environment
Recommended prior learning: None
Corequisites: None
Barred combinations: None
Professional body requirements: N/A
Module status: Core (BScSFC)

Module aims:
To address the concepts and principles of operating systems and the mechanisms used by operating systems to share information. To provide an understanding of facilities offered by modern operating systems. To explore the security features and vulnerabilities of operating systems. To examine the relationships between operating systems and networks, and the security aspects of these.

Module synopsis:
The module addresses the basic problems of the allocation, management and protection of computing resources in single and multi-user systems, single processor and networked systems. It will provide learners with an understanding and perspective of security strengths and weaknesses in both stand alone and networked operating systems. Methods of improving the security of computers through both standard features of operating systems and additional software interacting with operating systems will be explored. Standards for formally proven security will be studied.

Learning Outcomes:

1. Knowledge Outcomes

Upon completion of this module the student will understand:
1.1 The principles of resource allocation and management in computer systems.
1.2 Both classic and modern operating system structures.
1.3 The need and rationale for security and the mechanisms used to provide it.
1.4 Current and historical solutions to these problems
1.5 The techniques used to establish operating system and network security.

2. Ability Outcomes

Upon completion of this module the student will be able to:
2.1 Obtain operating system performance measurements and explain the reasons for underperformance.
2.2 Configure the security features of an operating system and test it to establish its security level.
2.3 Determine the effects of security policies.
2.4 Use additional software to verify and manage system security.

Outline syllabus of topics to be covered:

- Operating System (OS) structures
- Processes threads and concurrency
- Memory management - virtual memory, paging and segmentation
- Scheduling
- File systems and I/O
- Networks and Distributed Systems/Processing
- Client/Server architectures and Object based solutions
- User Interfaces and command interpreters
- Security issues
- OS development tools
- User identity and access control
- OS vulnerability and process control
- Optional facilities of an OS relevant to security
- Methods of testing an OS for security
- Additional security software and hardware
- Network security and monitoring
- OS and network logs and traceability
- Cryptographic and penetration testing

Indicative learning strategy:
The theoretical framework for the first part of the course will be based on a layered O/S model with each layer providing an interface to the layer above, combined with the notion of providing a virtual machine for user process to run in. This model will be compared and contrasted with the approaches taken by real systems. The main systems examined will be UNIX/Linux; and Windows; other systems will be used to cover topics such as microkernel architectures (Mach & plan9) or distributed file systems and threads (Solaris). Security issues in both operating systems and networks will be considered from a theoretical perspective as well as by practical experiences where resources permit.

Indicative references/learning materials:

Ritchie, C	Operating Systems incorporating UNIX and Windows Letts, 1997, 3rd edition
Stalling, W	Operating Systems, Internals and Design Principles Prentice Hall, 1998
Silberschatz, Galvin	Operating Systems Concepts Addison Wesley, 1998
Gollmann, Dieter	Computer Security Wiley, 1999
Poole, Owen	Network Security, a Practical Guide Butterworth Heinemann, 2003

Also - various internet sources

Resources required:
The tutorial/practical period requires the use of a (Unix/linux/PC) computing laboratory with suitable local networking to enable real-world experiences of the subject as well as suitable simulation software. Approximately 50 per cent of the unsupervised study will be taken up in the computing laboratory.

Assessment strategy:
Assessment will be by one coursework (50%) and one two hour exam (50%). The coursework will assess outcomes 2.1 to 2.4. The exam will measure the outcomes 1.1 to 1.5.