MODULE **DESCRIPTOR**

MODULE TITLE	Computer Systems and Security		
MODULE CODE	CO1508 (L4)	CREDIT VALUE	20 credits / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

Gradually, we are becoming more and more dependent on computing systems in our daily lives. The services provided by these systems, such as online shopping, social networking, mobile banking and so forth represent the backbone of modern communities. Smart cities, Internet of Things (IoT), smart vehicles, and smart grids are a few examples of emerging technologies that will shape the future for coming generations.

Users anticipate these systems to operate exactly as expected and for their services to be secure and available whenever required. Systems damage or data loss through accident or malicious attacks can have serious implications including financial losses and even loss of lives.

In such a complicated eco-system, achieving computer systems security and services availability is no longer the responsibility of computer security specialists. In fact, it is a challenge that spans across all disciplines in computing. For instance, software engineers, game developers and information systems engineers ought to implement secure software systems to ensure their reliability and robustness against attacks such as game cheating and SQL injection. Moreover, network engineers must consider security measures when building a network to defend and mitigate against various attacks such as Denial of Service (DoS) and malware. Finally, forensics investigators should be aware of the current security measures/attacks to investigate the situation and assess the data breach.

To tackle this multidisciplinary challenge, it is of great importance to develop an understanding of the different parts of computer systems, their functions, how they are integrated and their vulnerabilities: this includes computer system architecture, operating systems, computer networks, human element in those systems, possible threats, and systems security.

This module aims to:

1. Explore the fundamentals of computer architecture and operating systems.
2. Examine a range of recent security threats and data breaches, their consequences on businesses and potential countermeasures.
3. Create awareness of the importance of complying with law, ethical and privacy issues regarding any collected data.
4. Discuss recent technologies and their emerging security problems.

Make students mindful of their computer security behaviour.

MODULE **CONTENT**

Computer System Components/Architecture

Top level view of computer functions and interconnection including computer components (e.g. CPUs, Primary/Secondary/Cache Memory, I/O devices), application programs and users.

Operating Systems Concepts

What Operating Systems (OSs) do? Process/Memory/Storage Management, Process Synchronisation, Concurrency, Transactions Management, Deadlocks, File Systems and Hardware Virtualisation.

Key Concepts of Protection and Security

Legal issues, Privacy and Ethics (e.g. Legal requirements such as Data Protection Act, Computer Misuse Act, the right to privacy, the ethics of accessing materials without the necessary authority). Foundations of Computer Security (Confidentiality, Integrity, Availability, Accountability, Non-repudiation, Reliability), Computer Security Objectives, Security Management (Policies, Measures etc.), Risk & Threat Analysis (Assets, Threats, Vulnerabilities, Attacks).

Security Tools

Identification and Authentication, Access Control (User-Centred Security Approach), Cryptography as a tool (Symmetric/Asymmetric Encryption, Digital Signatures, Secure Hashing), Firewalls, Detection, Prevention and Recovery Mechanisms, Aftermath (Digital Forensics for investigating, monitoring and preventing)

Introduction to Computing Systems Security

A subset of the following topics will be considered, depending on topical issues: Linux OR Windows Security, Database Security, Web Security, Mobile Phone Security, Social Network Security and Privacy issues and Wireless Network Security.

Emerging Technologies Security, Privacy and Ethical issues

A subset of the following topics will be considered, depending on topical issues: Smart City security (e.g., recent hacks against smart vehicles), IoT Security, Smart Grids Security, and more as new emerging technologies come under attacks every day.

INTENDED **LEARNING OUTCOMES**

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

1.	Explain the various components of operating systems and their roles.
2.	Compare different security threats affecting different computing systems and propose suitable countermeasures.
3.	Describe different tools and techniques to secure a computing system against specific threats.
4.	Evaluate the legal, social and ethical implications of a range of situations.

TEACHING METHODS

The module examines a useful range of the fundamental aspects of computer systems and security. Lectures will be delivered on campus to provide the formal taught content including concepts, techniques and information without digging into the mathematical details of some tools (e.g., cryptography).

The practical/tutorial sessions supplement and support the lectures allowing a discovery approach to learning.

Students are expected to engage in research activities for case studies and latest news of security breaches and hacks. URLs that contain relevant research material will be provided to the students in support of the syllabus. Students will prepare and share summaries of technologies and system components.

Students will discuss case studies and explore implications: e.g. considering commercial issues (e.g. “How much security is enough?”), ethical issues (e.g. “Is it ethical to crack copy protection?”), legal issues (e.g. “Can I connect to my neighbour’s WiFi?”), and social issues (e.g. “Should governments engage in cyber-warfare?”)

The assessment is designed to assess both the students’ comprehension of theoretical topics relevant to computer systems and security and their practical skills in tools and methods needed to achieve computing systems security. This also includes evaluation/assessment of recent security/data breaches and how to deal with them.

ASSESSMENT METHODS

This module is assessed through a Summary of investigation (e.g. as a Poster) (50%) and a report (50%).