WM183-15 Computer Architecture & Operating Systems

25/26

Department
WMG
Level
Undergraduate Level 1
Module leader
Hany Atlam
Credit value
15
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Computer architecture and operating systems are crucial for providing a deep understanding of how computers function at a fundamental level. This knowledge is essential for effectively designing, developing, and troubleshooting software applications. It helps in optimizing performance, identifying bottlenecks, and ensuring efficient resource utilization. Studying computer architecture and operating systems from a cyber security perspective helps gain insights into the vulnerabilities that arise from design choices, implementation flaws, or misconfigurations. It also allows the development of effective security measures and countermeasures to protect computer systems from attacks.
This module starts by providing essential principles and concepts of computer systems to develop a deeper understanding of the hardware environment upon which all computing is based, and the interface it provides to higher software layers. Students will learn about computer systems' functional components, their characteristics, performance, and interactions, and the challenge of harnessing parallelism to sustain performance improvements now and in the future. This module then outlines the principles of how an operating system is constructed, how it works, and its critical role in cyber security by providing a solid understanding of how a modern operating system satisfies its requirements in the cyber context.

Module aims

This module aims to equip students with a comprehensive understanding of modern computer architectures and system software concepts. The module starts by providing essential principles of computer architecture, providing insights into the fundamental components that represent computer systems. Then, the module progresses to the principles of how an operating system is designed and implemented highlighting its core mechanisms and functionalities. The module allows students to gain valuable insights into the essential intersection of computer systems, operating systems, and cyber security, enabling them to effectively analyse, design, and implement secure systems.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Outline content
The content of this module will be taught from a cyber security perspective.

- Digital logic and digital systems
- Machine-level representation of data
- Assembly-level machine organisation
- Memory system organisation and architecture
- Overview of operating systems
- Operating system principles
- Concurrency and synchronisation
- Scheduling and dispatch
- Memory management
- Security and protection
- File systems
- Interaction and network communication

Learning outcomes

By the end of the module, students should be able to:

- Understand the key architectural components of computer systems and essential principles behind the organisation and operation of a typical general-purpose operating system.
- Explain how simple processes, memory and file management algorithms and data structures work.
- Evaluate code at the assembly language level to analyse cyber consequences arising from insecure patterns of code.
- Select and effectively apply security measures and protection mechanisms

Indicative reading list

Stokes, Jon, “Inside the Machine: An Illustrated Introduction to Microprocessors and Computer Architecture”, No Starch Press (2015)

Love, Robert, “Linux System Programming: Talking Directly to the Kernel and C Library”, 2 Ed, O'Reilly (2013)

Silberschatz, Abraham, Galvin, Peter B., Gagne, Greg, “Operating System Concepts”, 9 Ed, Wiley (2013)

Tanenbaum, Andrew S., Bos, Herbert, “Modern Operating Systems”, 4 Ed, Pearson (2014)

Subject specific skills

Performance Optimization
Troubleshooting and Debugging
Exploitation of low-level coding vulnerabilities

Transferable skills

Problem solving and critical thinking

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours (24%)
Private study	54 hours (36%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Independent activity between workshops.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
In-class Test	20%	12 hours	No
This test is to assess student knowledge about components of computer systems and essential principles behind the operation of a typical general-purpose operating system.			
Coursework	80%	48 hours	Yes (extension)
Students will prepare a report to assess their understanding of the essential operation of the operating system as well as evaluate code at the assembly language level to analyse cyber consequences arising from insecure patterns of code and suggest appropriate security measures.			

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Solutions provided to tutorial questions
Summative feedback on assignments and exam

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security