WM140-18 Cyber Systems Architecture and Organisation

24/25

Department
WMG
Level
Undergraduate Level 1
Module leader
Hany Atlam
Credit value
18
Module duration
30 weeks
Assessment
50% coursework, 50% exam
Study location
University of Warwick main campus, Coventry

Description

Introductory description

In cyber security it is essential not to regard the computer as just a black box that executes programs by magic. The underlying hardware and software infrastructure upon which applications are constructed is collectively described by the term "computer systems." Computer systems broadly span the sub-disciplines of operating systems, parallel and distributed systems, communications networks, and computer architecture. These sub-disciplines share important common fundamental concepts including computational paradigms, parallelism, cross-layer communications, state and state transition, resource allocation and scheduling, and so on.

This module gives broad coverage to computer systems and develops a deeper understanding of the hardware environment upon which all computing is based, and the interface it provides to higher software layers. Students learn of a computer system’s functional components, their characteristics, performance, and interactions, and the challenge of harnessing parallelism to sustain performance improvements now and into the future. Students need to understand computer architecture to develop programs that can achieve high performance through a programmer’s awareness of parallelism and latency. In selecting a system to use, students should be able to understand the trade-off among various components, such as CPU clock speed, cycles per instruction, memory size, and average memory access time and how this influences cyber

security.

Module aims

The module aims to equip students with a comprehensive understanding of the fundamental components of computer systems, including hardware, software, and firmware, and their respective roles within a cyber system. The module aims to explain the relationship between abstractions used to represent programs and data and their concrete representation on real machines. Students will learn to identify and explain common vulnerabilities in computer systems architecture and how these can be exploited, as well as potential vulnerabilities in system architecture and propose effective mitigation strategies. Additionally, the module will equip students with the skills to evaluate code at the assembly language level, enabling them to analyse and address cyber consequences arising from insecure coding patterns.

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
- interfacing and communication
- computational paradigms
- parallelism
- evaluation
- proximity

Learning outcomes

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

- Explain the basic components of computer systems, including hardware, software, and firmware, and their roles in a cyber system. [CITP 2.1.1]
- Explain the relationship between the abstractions used to represent programs and data, and their concrete representation on real machines. [CITP 2.1.2]
- Explain the relationship between the key architectural components of a modern, multicore processor. [CITP 2.1.2] [AHEP4 C4]
- Explain and identify common vulnerabilities in computer systems architecture and how they can be exploited. [CITP 2.1.10]
- Evaluate code at the assembly language level to analyse cyber consequences from insecure patterns of code. [CITP 2.1.12] [AHEP4 C12]

Indicative reading list

Intel, “Intel 64 and IA-32 Architectures Software Developer Manuals”, https://software.intel.com/en-us/articles/intel-sdm [updated Dec 29 2016]

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

Tanenbaum, Andrew S., “Structured Computer Organisation”, 6 Ed, Pearson (2012)

Duntemann, Jeff, "Assembly Language Step-by-Step: Programming with Linux", 3 ed, Wiley (2009)

View reading list on Talis Aspire

Subject specific skills

Students will be able to:

- Develop skills in identifying and analysing the basic components of computer systems, including hardware, software, and firmware, and their roles within a cyber system.
- Develop the capability to identify potential vulnerabilities in system architecture and propose effective mitigation strategies.
- Develop the capability to evaluate code at the assembly language level to analyse cyber consequences resulting from insecure coding patterns.
- Engage in practical exercises to apply theoretical knowledge to real-world cyber security scenarios, strengthening problem-solving and analytical skills.

Transferable skills

Problem solving
Critical and Analytical Skills
Teamwork and collaboration
Communication skills

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (10%)
Supervised practical classes	18 sessions of 1 hour 30 minutes (15%)
Online learning (independent)	15 sessions of 1 hour (8%)
Private study	40 hours (22%)
Assessment	80 hours (44%)
Total	180 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming 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 C5

	Weighting	Study time
Coursework	50%	40 hours
Students will prepare a written report to assess their understanding of cyber system architecture, tools, and techniques within a specific scenario.		
Online Examination	50%	40 hours
To assess student understanding of cyber system architecture, tools, and techniques and apply theoretical knowledge to real-world cyber security scenarios.		

~Platforms - AEP

- Online examination: No Answerbook required

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Solutions provided to tutorial questions

Past exam papers for WM140

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