WM140-18 Cyber Systems Architecture and Organisation

23/24

Department
WMG
Level
Undergraduate Level 1
Module leader
Christo Panchev
Credit value
18
Module duration
30 weeks
Assessment
Multiple
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

Explain the relationship between the abstractions used to represent programs and data, and their concrete representation on real machines.
Explain the relationship between the key architectural components of a modern, multicore processor.
Evaluate code at the assembly language level to analyse cyber consequences from insecure patterns of code.

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 relationship between the abstractions used to represent programs and data, and their concrete representation on real machines.
- Explain the relationship between the key architectural components of a modern, multicore processor.
- Evaluate code at the assembly language level to analyse cyber consequences from insecure patterns of code.

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)

Subject specific skills

Apply theory to achieve desirable, practical cyber consequences.

Transferable skills

Problem solving

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 3 hours (56%)
Private study	42 hours (44%)
Total	96 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 C4

	Weighting	Study time
Coursework	50%	41 hours
Online Examination	50%	43 hours
~Platforms - AEP		

	Weighting	Study time

- Online examination: No Answerbook required

Assessment group R1

	Weighting	Study time
Resubmission coursework	100%	

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