WM242-24 Implementing Secure Systems

24/25

Department
WMG
Level
Undergraduate Level 2
Module leader
Sandy Taramonli
Credit value
24
Module duration
30 weeks
Assessment
60% coursework, 40% exam
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Secure systems have a singular goal - to concurrently enable things to happen that should happen, whilst preventing things from happening that should not happen. Within that simplicity are deep challenges: defining the contextually contingent sets of should and should not; anticipating what the future might bring; determining the extent of the system. Alongside these deep challenges however, there are well understood patterns of implementation that make the shoulds more likely and the should nots less likely. Similarly, there are well understood patterns that tend to encourage the opposite.

This module is concerned with deliberately choosing good patterns of implementation for the long-term well-being of the system under consideration.

Module aims

The aim of this module is to equip students with the knowledge and skills necessary to design, develop, and maintain secure systems. This includes understanding and applying best practices, employing core technologies, recognising security requirements and applying cryptographic techniques. The module also aims to enable students to construct comprehensive security

systems and evaluate their effectiveness, providing recommendations for future improvements.

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.

- Design and development considerations
- Selecting and applying core technologies
- Recognising security needs on, across and between platforms
- Cryptography
- Network security
- Human factors
- Security systems development

Learning outcomes

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

- To explore various methodologies and identify best practices in the design and development of secure systems.
- To select security measures specific to different platforms and understand how to implement secure communication between these systems.
- To employ appropriate core technologies to enhance system security according to the specified security requirements.
- To understand the principles of cryptography and apply cryptographic techniques for secure data storage and transfer.
- To construct and implement comprehensive security systems choosing the most effective security measures based on the given system requirements.
- To evaluate the security of the system and provide recommendations for future improvements.

Indicative reading list

Bray, S.W. (2020) Implementing Cryptography Using Python. Wiley

Computer security. Third (2011). Wiley Textbooks

Cryptography and network security: principles and practice. Eighth (2021). Pearson

Ferguson, N., Schneier, B. and Kohno, T. (2015) Cryptography Engineering. Wiley

View reading list on Talis Aspire

Subject specific skills

Technology Application, Cryptography, System Security, Secure System Design , Secure Systems

Development and evaluation

Transferable skills

Critical thinking, problem-solving, Technical report writing

Study

Study time

Type	Required
Supervised practical classes	45 sessions of 1 hour (19%)
Private study	99 hours (41%)
Assessment	96 hours (40%)
Total	240 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 must pass all assessment components to pass the module.

Assessment group D

	Weighting	Study time
Assignment 1	60%	56 hours

Students are given a scenario and are required to design a cryptosystem, implement it and write a report to present the proposed system. Students will need to justify the selection of the methods used and submit a functioning program along with the relevant documentation.

Assignment 2	40%	40 hours

Students are given a system and are required to evaluate it in terms of the security characteristics and make recommendations for improvements in the effectiveness of the system.

	Weighting	Study time
~Platforms - WAS		

- Online examination: No Answerbook required

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Summative feedback on assignments

Past exam papers for WM242

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security