

WM286-15 Secure Software Development

27/28

Department

WMG

Level

Undergraduate Level 2

Module leader

Bharath Sadasivaiah

Credit value

15

Module duration

10 weeks

Assessment

60% coursework, 40% exam

Study location

University of Warwick main campus, Coventry

Description

Introductory description

Software engineering is concerned with the application of theory, knowledge, and practice to effectively and efficiently build reliable and secure software systems that satisfy the requirements of customers and users. This discipline is applicable to small, medium, and large-scale systems. It encompasses all phases of the lifecycle of a software system, including requirements elicitation, analysis and specification; design; construction; verification and validation; deployment; and operation and maintenance. Whether small or large, following a traditional plan-driven development process, an agile approach, or some other method, software engineering is concerned with the best way to build good software systems. This module will look at software engineering in the context of cyber security, applying frameworks such as Trustworthy Software Framework, Secure Software Development Life Cycle. when developing software systems.

There is a specific focus on the security of software.

Module aims

This module aims to equip students with the knowledge and practical experience of secure software design and development principles.

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.

Software processes

Software project management

Tools and environments to support and manage:

Requirements engineering

Software design

Software construction

Software verification and validation

Software evolution in the context of large, pre-existing code bases

Software reliability

Software weaknesses

Case studies in software security and weaknesses

Secure software development

Learning outcomes

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

- Apply cyber security best practices across key phases of the software engineering lifecycle. [CITP 2.1.5, 2.1.6, 2.2.4]
- Demonstrate the understanding and application of relevant software development frameworks to a given software development scenario. [CITP 2.1.4, 2.1.6, 2.2.4, 2.2.6]
- Analyse and compare different methodologies for improving software and system security. [CITP 2.1.7, 2.2.2]
- Implement strategies and practices to enhance the security of software systems. [CITP 2.1.7, 2.2.4, 2.2.6]

Indicative reading list

[Reading lists can be found in Talis](#)

[Specific reading list for the module](#)

Subject specific skills

Advanced applied understanding of Secure software design, Secure software development
Software security testing and validation

Transferable skills

Problem Solving

Analytical Reasoning

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	10 sessions of 2 hours (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Additional lab work and research.

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	Eligible for self-certification
Assessment component			
Software Development and Individual Report	60%	36 hours	Yes (extension)
Students are presented with a scenario and tasked with designing a secure software system, implementing it, and producing a report to present their proposed solution. They must justify their choice of methods, submit a functioning program with supporting documentation, and apply cyber security best practices throughout the software engineering lifecycle.			

	Weighting	Study time	Eligible for self-certification
Reassessment component			
Software Development and Individual Report			No
Students are presented with a scenario and tasked with designing a secure software system, implementing it, and producing a report to present their proposed solution. They must justify their choice of methods, submit a functioning program with supporting documentation, and apply cyber security best practices throughout the software engineering lifecycle.			

Assessment component

Exam	40%	24 hours	No
Students are provided with a software system and are required to evaluate its security features, identifying potential improvements and making recommendations to enhance end-to-end system security.			

Only resources to be used are authorised in class notes.

~Platforms - WAS

-
- Online examination: No Answerbook required

Reassessment component is the same

Feedback on assessment

Written feedback for each report, verbal feedback during sessions.

For the exam, a per-question breakdown of students' marks, together with any marker comments, may be given.

[Past exam papers for WM286](#)

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