WM242-24 Implementing Secure Systems

22/23

Department
WMG
Level
Undergraduate Level 2
Module leader
Peter Norris
Credit value
24
Module duration
30 weeks
Assessment
Multiple
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

1 – Reason about the relationship between human trust and the technological tokens that represent trust in cyber systems.
2 - Design a security architecture that satisfies the security needs of a given scenario.

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:

- 1 – Reason about the relationship between human trust and the technological tokens that represent trust in cyber systems.
- 2 - Design a security architecture that satisfies the security needs of a given scenario.
- 3 - Configure systems, applying cryptographic techniques as needed, to achieve desired security objectives.

Indicative reading list

Bejtlich, Richard, “The Practice of Network Security Monitoring”, No Starch Press (2013)

Merkow, Mark S. and Raghavan, Lakshmikanth, “Secure and Resilient Software Development”, Auerbach Publications (2010)

Stallings, William, “Cryptography and Network Security: Principles and Practice”, 7 Ed, Pearson (2016)

Subject specific skills

1 – Reason about the relationship between human trust and the technological tokens that represent trust in cyber systems.
2 - Design a security architecture that satisfies the security needs of a given scenario.
3 - Configure systems, applying cryptographic techniques as needed, to achieve desired security objectives.

Transferable skills

Critical thinking, problem solving

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours 30 minutes (19%)
Private study	66 hours (28%)
Assessment	129 hours (54%)
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 do not need to pass all assessment components to pass the module.

Assessment group A3

	Weighting	Study time	Eligible for self-certification
Assignment 1	20%	26 hours	No
Assignment 2	35%	45 hours	No
Assignment 4	40%	52 hours	No
Assignment 3	5%	6 hours	Yes (extension)

Assessment group R

	Weighting	Study time	Eligible for self-certification
Coursework	100%		Yes (extension)

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions

Summative feedback on assignments

Availability

Courses

This module is Core for:

- Year 2 of UWMA-H651 Undergraduate Cyber Security