Module Specification

Security Assurance

Version: 2023-24, v2.0, 19 Jul 2023

Contents

Part 1: Information

Module title: Security Assurance

Module code: UFCFLU-30-3

Level: Level 6

For implementation from: 2023-24

UWE credit rating: 30

ECTS credit rating: 15

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field:

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: There are recognised IT security design principles which can be applied to IT systems and software. A security case is a body of evidence that demonstrates that a system is secure. These include assessing security architectures that incorporate hardware and software components. A security case should take these principles and architectures into account and include:

A clear definition of the security objectives of the case

Threats that are likely to exist against the target system (physical, intrusion, malware)
Risks to the system, measured in probabilities (very likely, likely and unlikely)
Potential impact / severity (major, moderate, minor)

These security design principles will be explored and instantiated in this module.
Strategies for dealing with risks (avoid, accept, mitigate, transfer)

Features: Not applicable

Educational aims: In this module students are applying their knowledge of cyber security concepts and principles in an autonomous, professional manner.

Outline syllabus: You will cover:
composing a security case, deriving objectives with reasoned justification in a representative business scenario

interpreting security policy and risk profiles into secure architectural solutions that meet security objectives, mitigate the risks and conform to legislation in a representative business scenario

fundamental security technology building blocks and typical architectures and architecture frameworks

design principles for architecting a secure system, for example
- separation of concerns, fail-safe/fail-secure, defence in depth, least privilege
- application of proven security architectural patterns from reputable sources
- incorporation of appropriate security controls

security assurance and how an architecture may be assured
security assurance:
- role in cyber security
- ‘trustworthy’ versus ‘trusted’
- assurance of an architecture

approaches to assurance
- intrinsic, extrinsic, design and implementation, operational policy and process
- examples of how these might be applied at different stages in the life-cycle of a

system.

at least one current system of extrinsic assurance

e.g., red teaming (penetration testing), security testing, supply chain assurance, Common Criteria

benefits and limitations

third party testing (e.g., ethical hacking) and how it contributes to assurance

at least 2 ways an organisation can provide intrinsic assurance

Part 3: Teaching and learning methods

Teaching and learning methods: Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Apply security principles and assurance in an organisation.

MO2 Apply design principles for architecting a secure system.

MO3 Develop a security case for an organisation, using recognised methods and to an internationally recognised standard.

MO4 Reflect on the process of developing a security case, justifying methods used and /or proposing alternatives.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/46ED1193-FEAF-9EF8-6231-DAA482E9CAAD.html

Part 4: Assessment

Assessment strategy: At both first sit and resit this module is assessed by:

A written, unseen, 2-hour exam will test the student's understanding of security assurance and architecting a secure system.

In the coursework, students apply their knowledge to a practical situation, either from their workplace or from a case study organisation. The coursework contextualises the underpinning knowledge and consolidates the connection between academic study and its application.

Students will develop and report on a security case, based on a given, or real (from their workplace) scenario. The work will be recorded in a workbook, along with a reflection.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: Practical workbook that records the development of a security case.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO4

Examination (First Sit)
Description: 2 hour exam to test underpinning knowledge.
Weighting: 50 %
Final assessment: No

Group work: No
Learning outcomes tested: MO1, MO2

Practical Skills Assessment (Resit)
Description: Practical workbook that records the development of a security case.
Weighting: 50 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO4

Examination (Resit)
Description: 2 hour exam to test underpinning knowledge.
Weighting: 50 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL}
[Sep][FT][GlosColl][3yrs] BSc (Hons) 2021-22