Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM760
Module Title	Secure Computing
Level	7
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GCAP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc Cyber Security	Core
MSc Cyber Security with Advanced Practice	Core
MSc Computer Science	Core
MSc Computer Science with Advanced Practice	Core

Pre-requisites

None

Breakdown of module hours

Learning and teaching hours	11 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	10 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**21** hrs
Placement / work based learning	0 hrs
Guided independent study	179 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2024

For office use only	
Date and details of revision	
Version number	1

Module aims

This module offers students a holistic understanding of key topics in computer security these may include;

- Risks & Threats
- Cryptography
- Secure software development principles
- Access control & Authentication
- Information security governance
- Security policy and risk management

Students will explore various aspects such as identifying vulnerabilities, encryption algorithms, secure coding practices, user authentication methods, establishing security policies, and effectively managing risks and incidents. This module equips students with the knowledge and skills necessary to navigate the complex field of computer security and to implement robust security measures in diverse technological environments.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Demonstrate the concepts, principles, and goals of secure computing.
2	Critically evaluate the risks and threats in the digital environment, implementing appropriate countermeasures.
3	Apply cryptographic techniques to ensure data confidentiality, integrity, and authenticity.
4	Implement secure software development principles and practices, mitigating common vulnerabilities and ensuring the creation of robust and secure applications.

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The portfolio could assess tasks such as designing/implement a cryptographic solution for a specific scenario, ensuring data confidentiality, integrity, and authenticity. Providing a detailed explanation of the cryptographic techniques employed and evaluate their effectiveness in safeguarding sensitive information.

Developing a secure software application following best practices and secure coding principles. Mitigating common vulnerabilities, such as injection attacks and cross-site scripting, through appropriate coding techniques, input validation, and output encoding. Providing evidence of robust testing and validation to ensure the security of the application.

By undertaking these assessments, students can demonstrate their understanding of secure computing concepts, their ability to evaluate and mitigate risks, apply cryptographic techniques, and implement secure software development principles. These tasks enable students to showcase their proficiency in creating secure computing environments and applications.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Indicative Syllabus Outline

- Risks and Threats
  - Identification and classification of risks
  - Risk assessment methodologies and frameworks
  - Understanding the impact and likelihood of various threats
  - Developing risk mitigation strategies and incident response plans
- Cryptography
  - Symmetric and asymmetric encryption algorithms
  - Hash functions, digital signatures, and their role in ensuring data integrity and authenticity
  - Key management, including key generation, distribution, and storage
  - Application of cryptography in securing communication channels
- Secure Software Development Principles
  - Input validation, output encoding, and secure error handling
  - Mitigating common software vulnerabilities, such as injection attacks, cross-site scripting (XSS), and cross-site request forgery (CSRF)
  - Security-focused software development methodologies
  - Code review, testing, and static analysis tools for identifying security flaws
- Access Control and Authentication
  - Authentication mechanisms, multifactor authentication and biometrics
  - Access control lists (ACLs)
  - User provisioning and privilege management
  - Identity and access management (IAM) systems
- Information Security Governance
  - Governance frameworks, standards, and regulations related to information security

- Risk Management
  - Auditing and assessing security to ensure compliance and mitigate risks
  - Developing and implementing security policies and procedures

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, and Dwayne Williams. *Principles of Computer Security, CompTIA Security+ and Beyond.* McGraw-Hill Education, 2021.

Other indicative reading

W. Stallings., & L .Brown, *Computer Security: Principles and Practice*. Pearson, 2018.

R Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley, 2021

B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley,2017.

C. Kaufman, R. Perlman, & M. Speciner, *Network Security: Private Communication in a Public World.* Pearson, 2022.