CS2D6-15 Cyber Security (DA)

22/23

Department
Computer Science
Level
Undergraduate Level 2
Module leader
Andrew Hague
Credit value
15
Module duration
5 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

This module will enable students to understand basic concepts of computer security, including common security threats and measures to combat them. This will enable them to demonstrate an appreciation of the practical aspects of computer (in)security, critical analysis with respect to the evaluation of system security, and skills appropriate to the computer science professional in the assessment and design of secure systems. They will then go on to apply this knowledge to analyse and inform aspects of their security practice that apply particularly to their specific area of work.

Module aims

This module aims to:

- introduce the fundamental concepts and themes of computer security and provide a grounding in some of the main ideas and concerns in this area
- provide practical experience of applying knowledge in this area to security issues in practice
- develop students' understanding of how these topics apply and are managed in their own workplace
- enable students to analyse and inform aspects of security practice that apply particularly to their specific area of work

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.

This module consists of:

Introduction to basic computer security

- Important concepts in security (basic definitions, security threats, risk assessment, practical measures (e.g. identification, authentication, audit trails))
- Security models
- Basics of cryptography
- Network security

Security in practice

- The development of secure systems
- Introduction to relevant security features and technologies

Learning outcomes

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

- Demonstrate knowledge of key computer security concepts and of the challenges to computer security.
- Understand common security threats and have a basic knowledge of measures to combat them.
- Demonstrate knowledge of different approaches to risk assessment.
- Demonstrate understanding of key network security issues, e.g. password management, authentication, and access control.
- Understand basic theoretical features of secret key and public key cryptography and key standards and algorithms that implement them.
- Understand the use of cryptographic techniques in network security, e.g. features of security protocols, key exchange, key management, authentication, etc.
- Assess, analyse, and mitigate against risk in the context of their own workplace.
- Demonstrate critical analysis with respect to the evaluation of system security.
- Demonstrate knowledge of some of the key aspects of secure system design and programming language features.
- Demonstrate skills appropriate to the computer science professional in the assessment and design of secure systems.

Indicative reading list

Stallings, W., "Cryptography and Network Security (4/e)", Pearson (2006)
Mollins, R., "Introduction to Cryptography (2/e)" (2007)
Kaufman, C., "Network Security (2/e)", Perlman and Speciner (2002)
Schneier, B., "Secrets and Lies", Wiley (2004)

Anderson, R., "Security Engineering (2/e)", Wiley (2008)
Gollman, D., "Computer Security (3/e)", Hoboken (2011)

Subject specific skills

- Analyse business and technical requirements to select and specify analyses business and technical requirements to select and specify appropriate technology solutions
- Manage the development and assurance of software artefacts applying secure development practises to ensure system resilience
- Perform database administration tasks and is cognisant of the key concepts of data quality and data security
- Can undertake a security risk assessment for a simple IT system and propose resolution advice
- Can identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. Cloud services)
- Identify network security risks and their resolution.
- Common vulnerabilities in computer networks including unsecure coding and unprotected networks

Transferable skills

- Have demonstrated that they have mastered basic business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality.
- Flexible attitude
- Ability to perform under pressure
- A thorough approach to work

Study

Study time

Type	Required
Lectures	15 sessions of 1 hour (10%)
Tutorials	14 sessions of 1 hour (9%)
Practical classes	9 sessions of 2 hours 30 minutes (15%)
Work-based learning	157 sessions of 30 minutes (52%)
Online learning (independent)	20 sessions of 1 hour (13%)
Total	150 hours

Private study description

No private study requirements defined for this module.

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 C

	Weighting	Study time
Cyber Security	50%	
Reflective report of workplace learning activity	50%	

Feedback on assessment

Written and verbal

Availability

There is currently no information about the courses for which this module is core or optional.