

CS263-15 Cyber Security

23/24

Department

Computer Science

Level

Undergraduate Level 2

Module leader

Khalil Challita

Credit value

15

Module duration

10 weeks

Assessment

Multiple

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module introduces students to several key aspects of cyber security as well as spreading awareness of the current cyber security landscape and threat actors.

Module aims

The module provides students with a good understanding of technical aspects of cyber security to help them, among other things, to identify vulnerabilities and weaknesses in computer systems, networks, and applications.

This module also underlines the importance of risk assessment, compliance, and contingency planning to help upper management make the right decisions in order to manage risks, protect sensitive data, and minimise legal and financial consequences in case of a data breach.

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 covers both technical and non-technical aspects of cyber security.

After a brief introduction to the field of cyber security, students should learn more about the below

topics.

- Penetration testing using Kali Linux
- Web application testing
- Fuzzing
- Social engineering attacks
- Open Source Intelligence techniques
- Program security
- Threat modelling
- Governance, risk management, compliance
- Risk assessment
- Contingency planning

Note that all labs can be performed on the DCS machines where several Virtual Machines (VMs) have been installed for this purpose.

Learning outcomes

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

- Test the security of a computer network.
- Test the security of a web application.
- Design a secure program by avoiding common programming mistakes that lead to unsecure applications.
- Use OSINT techniques to geolocate an image.
- Identify and assess the risks associated to an application, a computing system, or a company.
- Be aware of common standards and regulations to help senior management make strategic decisions.

Indicative reading list

Non-compulsory reading list:

- 1- Cybersecurity – Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system, 3rd Edition, by Diogenes and Ozkaya, Packt Publishing, 2022
- 2- The web application hacker handbook, 2nd edition, by Stuttard and Pinto, Wiley, 2011
- 3- Management of Information Security, Sixth Edition, M. Whitman, H. Mattord, 2018
- 4- Secrets and Lies: Digital Security in a Networked World, Bruce Schneier, 2004

[View reading list on Talis Aspire](#)

Subject specific skills

See syllabus

Transferable skills

Technical skills;
Communication skills;
Critical thinking;
Multitasking;

Study

Study time

Type	Required
Lectures	30 sessions of 1 hour (20%)
Supervised practical classes	10 sessions of 1 hour (7%)
Private study	110 hours (73%)
Total	150 hours

Private study description

Background reading of recommended texts.
Work on unsupervised practical assignment
Exam revision

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Students can register for this module without taking any assessment.

Assessment group D4

	Weighting	Study time	Eligible for self-certification
Unsupervised practical assignment	30%		No

Unsupervised practical assignment. This assignment is worth more than 3 CATS and is not,

	Weighting	Study time	Eligible for self-certification
therefore, eligible for self-certification.			
Examination CS263 Exam	70%		No

- Answerbook Pink (12 page)

Assessment group R3

	Weighting	Study time	Eligible for self-certification
Examination CS263 resit exam	100%		No

- Answerbook Pink (12 page)

Feedback on assessment

Written Feedback given via Tabula

[Past exam papers for CS263](#)

Availability

Pre-requisites

This module is only available to students in the second year of their degree and is not available as an unusual option to students in other years of study.

Courses

This module is Optional for:

- Year 2 of UCSA-I1N1 Undergraduate Computer Science with Business Studies

This module is Option list A for:

- Year 2 of UCSA-G500 Undergraduate Computer Science
- UCSA-G503 Undergraduate Computer Science MEng

- Year 2 of G500 Computer Science
- Year 2 of G503 Computer Science MEng

This module is Option list B for:

- Year 2 of UCSA-G4G1 Undergraduate Discrete Mathematics
- Year 2 of UCSA-G4G3 Undergraduate Discrete Mathematics