Swansea University
Prifysgol Abertawe

FACULTY OF SCIENCE AND ENGINEERING

POSTGRADUATE STUDENT HANDBOOK

MSC (FHEQ LEVEL 7)

CYBER SECURITY

DEGREE PROGRAMMES

SUBJECT SPECIFIC
PART TWO OF TWO
MODULE AND COURSE STRUCTURE
2023-24

DISCLAIMER

The Faculty of Science and Engineering has made all reasonable efforts to ensure that the information contained within this publication is accurate and up-to-date when published but can accept no responsibility for any errors or omissions.

The Faculty of Science and Engineering reserves the right to revise, alter or discontinue degree programmes or modules and to amend regulations and procedures at any time, but every effort will be made to notify interested parties.

It should be noted that not every module listed in this handbook may be available every year, and changes may be made to the details of the modules. You are advised to contact the Faculty of Science and Engineering directly if you require further information.

The 23-24 academic year begins on 25 September 2023

Full term dates can be found here

DATES OF 23-24 TERMS

25 September 2023 – 15 December 2023

8 January 2024 – 22 March 2024

15 April 2024 – 07 June 2024

SEMESTER 1

25 September 2023 – 29 January 2024

SEMESTER 2

29 January 2024 – 07 June 2024

SUMMER

10 June 2024 – 20 September 2024

IMPORTANT

Swansea University and the Faculty of Science of Engineering takes any form of **academic misconduct** very seriously. In order to maintain academic integrity and ensure that the quality of an Award from Swansea University is not diminished, it is important to ensure that all students are judged on their ability. No student should have an unfair advantage over another as a result of academic misconduct - whether this is in the form of **Plagiarism**, **Collusion** or **Commissioning**.

It is important that you are aware of the **guidelines** governing Academic Misconduct within the University/Faculty of Science and Engineering and the possible implications. The Faculty of Science and Engineering will not take intent into consideration and in relation to an allegation of academic misconduct - there can be no defence that the offence was committed unintentionally or accidentally.

Please ensure that you read the University webpages covering the topic – procedural guidance here and further information here. You should also read the Faculty Part One handbook fully, in particular the pages that concern Academic Misconduct/Academic Integrity.

Welcome to the Faculty of Science and Engineering!

Whether you are a new or a returning student, we could not be happier to be on this journey with you.

At Swansea University and in the Faculty of Science and Engineering, we believe in working in partnership with students. We work hard to break down barriers and value the contribution of everyone.

Our goal is an inclusive community where everyone is respected, and everyone's contributions are valued. Always feel free to talk to academic, technical and administrative staff, administrators - I'm sure you will find many friendly helping hands ready to assist you. And make the most of living and working alongside your fellow students.

During your time with us, please learn, create, collaborate, and most of all – enjoy yourself!

Professor David Smith
Pro-Vice-Chancellor and Executive Dean
Faculty of Science and Engineering

Faculty of Science and Engineering	
Pro-Vice-Chancellor and Executive Dean	Professor David Smith
Director of Faculty Operations	Mrs Ruth Bunting
Associate Dean – Student Learning and Experience (SLE)	Professor Laura Roberts
School of Mathematics and Computer Science	
Head of School	Professor Elaine Crooks
School Education Lead	Dr Neal Harman
Head of Computer Science	Professor Xianghua Xie
Computer Science Programme Director	Postgraduate Taught – Dr Bertie Müller
Coordinators	Advanced Computer Science – Dr Anton Setzer Advanced Software Technology – Dr Anton Setzer Computer Science (MSc) – Dr Oliver Kullmann Cyber Security – Dr Pardeep Kumar Data Science – Dr Alma Rahat

STUDENT SUPPORT

The Faculty of Science and Engineering has two **Reception** areas - Engineering Central (Bay Campus) and Wallace 223c (Singleton Park Campus).

Standard Reception opening hours are Monday-Friday 8.30am-4pm.

The **Student Support Team** provides dedicated and professional support to all students in the Faculty of Science and Engineering. Should you require assistance, have any questions, be unsure what to do or are experiencing difficulties with your studies or in your personal life, our team can offer direct help and advice, plus signpost you to further sources of support within the University. There are lots of ways to get information and contact the team:

Email: studentsupport-scienceengineering@swansea.ac.uk (Monday–Friday, 9am–5pm)

Call: +44 (0) 1792 295514 (Monday-Friday, 10am–12pm, 2–4pm).

Zoom: By appointment. Students can email, and if appropriate we will share a link to our Zoom calendar for students to select a date/time to meet.

The current student **webpages** also contain useful information and links to other resources:

https://myuni.swansea.ac.uk/fse/

READING LISTS

Reading lists for each module are available on the course Canvas page and are also accessible via http://ifindreading.swan.ac.uk/. We've removed reading lists from the 23-24 handbooks to ensure that you have access to the most up-to-date versions.
We do not expect you to purchase textbooks, unless it is a specified key text for the course.

THE DIFFERENCE BETWEEN COMPULSORY AND CORE MODULES

Compulsory modules must be **pursued** by a student.

Core modules must not only be **pursued**, but also **passed** before a student can proceed to the next level of study or qualify for an award. Failures in core modules must be redeemed.

Further information can be found under "Modular Terminology" on the following link - https://myuni.swansea.ac.uk/academic-life/academic-regulations/taught-guidance/essentialinfo-taught-students/your-programme-explained/

MSc (FHEQ Level 7) 2023/24
Cyber Security
MSc Cyber Security

Coordinator: Dr P Kumar

Compulsory Modules

Semester 1 Modules	Semester 2 Modules
CSCM08 **Information Security Management** **15 Credits** **Dr B Muller**	**CSCM10** **Computer Science Project Research Methods** **15 Credits** **Dr MJ Roach**
CSCM13 **Critical Systems** **15 Credits** **Dr AG Setzer**	**CSCM28** **Security Vulnerabilities and Penetration Testing** **15 Credits** **Dr JE Blanck**
CSCM18 **IT-Security: Cryptography and Network Security** **15 Credits** **Dr P Kumar/Dr E Neumann**	**CSCM88** **Network and Wireless Security** **15 Credits** **Dr P Kumar**
Dissertation	
CS-M20 **MSc Project** **60 Credits** **Dr U Berger** **CORE**	
Total 180 Credits	

Optional Modules

Choose exactly 15 credits

Graduates from our BSc programmes in Computer Science at Swansea University are usually not allowed to take modules of which they have already taken the level 3 version. The department aims to offer sufficient modules to allow a balanced choice of optional modules. In case of queries regarding the required modules for your scheme, please contact the course coordinator for the respective scheme.

Choose one module.

CSCM23	Designing-in Trust, Understanding and Negotiation	Dr B Muller/Prof M Roggenbach/Dr AZ Wyner/..	TB1	15
CSCM48	Web Application Development	Dr SP Walton	TB1	15
CSCM85	Modelling and Verification Techniques	Dr U Berger	TB1	15

And

Choose exactly 15 credits

Choose one module.

CSCM29	Blockchain, Cryptocurrencies and Smart Contracts	Dr AG Setzer	TB2	15
CSCM38	Advanced Topics: Artificial Intelligence and Cyber Security	Prof SA Shaikh/Prof J Zhang	TB2	15

CS-M20 MSc Project

Credits: 60 Session: 2023/24 September-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr U Berger

Format: Individual project supervision

Delivery Method: Individual project supervision

Module Aims: This module will provide students with the opportunity of exploring a particular topic in computer science in some considerable depth. It is only open to students studying MSc Computer Science, MSc Advanced Computer Science, MSc Advanced Software Technology, MSc in High Performance and Scientific Computing, and MSc Data Science.

Module Content: The student will carry out independent project under the guidance of their supervisor. The dissertation may include the
following topics:

- Discussion of the subject area and its history;
- A literature survey;
- Formulation of scientific questions and the answers to them;
- Theoretical background;
- Description of the approach taken;
- Discussion of issues arising in the undertaking of the project;
- Evaluation of results;
- Progress and achievements of the project;
- Suggestions for further work.

Intended Learning Outcomes: Students will be able
to undertake independent research into appropriate areas of Computer Science;
plan and undertake a significant independent piece of project work;
critically evaluate their work in the context of current work in related areas.

Assessment: Project (100%)

Assessment Description: Project dissertation. The maximum word count for a Swansea University MSc is defined in the online Academic Guide:
http://www.swan.ac.uk/registry/academicguide/

Moderation approach to main assessment: Universal Double Blind Marking of the whole cohort

Assessment Feedback: Students will receive guidance from their academic supervisor during individual supervision meetings. The minimum frequency of these is defined in University regulations; though it is expected that in practice they will be more frequent. Formal notification of the result of the MSc dissertation will be sent to the student via usual University processes. The student will receive individual feedback on their dissertation from their supervisor.

Failure Redemption: Resubmit dissertation in accordance with University regulations.

Additional Notes: Only available to students pursuing an MSc degree in Computer Science.

CSCM08 Information Security Management

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr B Muller

Format: 30 hours lectures and seminars

Delivery Method: On-campus lectures and lab sessions.

Module Aims: This module will address the theory and practice of information security. In particular, it will consider where data comes from, who collects it and what they can do with it. It will further look into theories of monitoring and surveillance, digital identity, legal and regulatory frameworks, data protection, cybercrime, business resilience, disaster recovery, and security audits.

Module Content: The theory and practice of information security: where does data come from, who collects it and what can they do with it? Data as a management tool, commodity, private asset, public good and public service.

Theories of monitoring and surveillance.

Theories of digital identity with applications to trust, anonymization and privacy. Technologies: biometrics, authentication, access control.

Legal and regulatory frameworks. Information Commissioners Office. Development of data protection. General Data Protection Regulation 2018. Company security policies and practices on digital media: use of email, the web and databases whilst at work, travelling and at home. Failures of information security: internal versus external. Case studies of data breaches.

The global landscape of cybercrime. Classification of cybercrime. Hackers and mules -- social engineering, leakage, penetration, betrayal, etc. Case studies of cybercrime, especially fraud. Convergence of real and virtual crimes.

Business resilience, continuity and disaster recovery. Risk analysis. Security audits. Role of chief information security officers.

Intended Learning Outcomes: Students will be able to
- critically evaluate the personal, organisational, and legal/regulatory context in which information systems could be used, the risks of such use and the constraints that may affect how cyber security is implemented and managed,
- explain security requirements, and specify appropriate security measures,
- critically analyse the nature, role and problems of data in all aspects of modern life as well as the scope and limits of technologies and human factors in security,
- carry out risk analysis and evaluate compliance issues for data in an organisation or company,
- undertake security audits of policies, practices and technologies.

Assessment:	Assignment 1 (30%)
	Examination (70%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Assignment 1: Short report and group presentation/video

The exam will be a regular closed-book 2h exam.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Formative feedback during term time. Written individual feedback on presentation and report outlining strengths and weaknesses.

Failure Redemption: Use of resit instrument as appropriate.

Additional Notes:

Available to visiting and exchange students.

CSCM10 Computer Science Project Research Methods

Credits: 15 Session: 2023/24 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr MJ Roach

Format: 12 lectures and seminars plus 6 one-to-one project supervision meetings; 3 hours presentations

Delivery Method: On-campus lectures

Module Aims: This module will introduce students to some fundamental research methodologies and good practice in research. They will undertake background research including a literature review and specify the aims of their MSc project.

Module Content: Seminars about selected scientific texts and research projects

Lectures on

- fundamental research methodologies
- good practice in research
- formulation of research questions and hypotheses
- logical reasoning
- literature research
- proper acknowledgement of sources
- principles of carrying out experimental research including ethical issues
- presentation of results

Individual guidance from project supervisors on

- identifying a research topic
- finding and reading related work
- report writing, citations and references
- using (digital) library services and search tools

Intended Learning Outcomes: Students will:-

- have gained a thorough understanding of fundamental research methodologies and good practice in research including:

- the formulation of research questions and hypotheses;
- techniques of valid and convincing argumentation;
- literature research methods;
- the proper acknowledgement of sources;
- the extraction of information from literature;
- project planning.

- be conversant with the principles of carrying out experimental research.
- have an understanding of how scientific research is conducted, reported, reasoned about and evaluated.
- be able to show their understanding of the requirements of a masters level project by writing a formal project proposal and specification which contains an outline solution to the problem and which clearly defines the scope of the MSc project, its goals, the methodology to be undertaken and the criteria of its evaluation
- have gained an in-depth knowledge in specific areas related to their project, and have critically assessed different methods to be used in their project and will have developed a detailed plan for carrying out their project.

have an understanding and appreciation of the importance of relevant legal, social, ethical and professional issues as they relate to their project.

Assessment:	Presentation (40%) Report (50%) Class Test 1 - Coursework (10%)
Resit Assessment:	Coursework reassessment instrument (100%)

Assessment Description: Initial Project Report - This report will be in the form of a technical academic report and consist of key contents: Project definition and evidence of understanding the challenges of the project.

Project Presentation - Presentation on the project at the Student Conference.

Moderation approach to main assessment: Universal Double Blind Marking of the whole cohort

Assessment Feedback: Individual feedback will be given by markers (CSCM10 lecturers, supervisors and second markers) using marking pro-forma. The comments and marks of the detailed specification document will be discussed by the project supervisor at individual meetings.

Failure Redemption: Failure to be redeemed by submitting a document addressing unsatisfactory aspects of initial submission(s) in the form of a project specification report or a project reflection report.

Additional Notes:

Only available to students on MSc Computer Science, MSc Advanced Computer Science, MSc Advanced Software Technology.

CSCM13 Critical Systems

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr AG Setzer

Format: 20 hours lectures, 10 hours lab.

Delivery Method: On campus lectures.

Module Aims: This module introduces techniques for developing critical systems, especially safety critical systems. Students will gain experience in applying modern tools in the development of critical software.

Module Content: Introduction and Motivation:
What are high integrity and critical systems? Legal and ethical issues. Examples of major failures of high integrity systems. Successes and how/why they worked. Standards for safety-critical software and their shortcomings.

Analysis:
The hazard analysis process. Safety analysis and the safety case. Safety issues related to, but outside software.
Human factors - the role of poor interfaces in software failures.

Specification and Verification:
Languages and tools for formal specification and verification of software. Detailed demonstration of one tool and its underlying theory.

Software Production:
Issues in program language selection to minimise failure. The software engineering process in the production of high-integrity software;

Correctness:
Validation and verification - the advantages and disadvantages of testing and formal verification.

Intended Learning Outcomes: Students will be thoroughly familiar with issues surrounding safety-critical systems, including legal and ethical issues and hazard analysis. They will understand techniques for specifying and verifying high-integrity software. They will have experience in applying formal specification techniques to critical systems. They will be familiar with and have had experience in applying programming languages suitable for developing high-integrity software for critical systems.

Assessment:	Examination 1 (60%)
	Coursework 2 (20%)
	Coursework 1 (20%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination, duration 2hrs.
The coursework consists of
Assignment 1 - Programming tasks
Assignment 2 - Case study

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Coursework: small report on strength and weaknesses of each solution.
Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam and/or resubmit assignments as appropriate.

Additional Notes: Available to visiting and exchange students.

CSCM18 IT-Security: Cryptography and Network Security

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr P Kumar, Dr E Neumann

Format: 30 hours lectures and labs

Delivery Method: On-campus lectures and lab sessions.

Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network security.

Module Content: Security threats and their causes.
Security criteria and models.
Cryptography: including basic encryption, DES, AES, hash functions.
Access Control.
Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools.
Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection.
Security issues in wireless networks.
Security on the cloud.

Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures.
Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis.
Students will synthesize the concepts of design, defensive programming, as well as their application to to build robust and resilient systems.
Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of the limits of these techniques.
Students will be able to reflect and critique on cryptographic techniques and secure systems design.

Assessment:	Examination 1 (70%)
	Coursework 1 (10%)
	Coursework 2 (10%)
	Laboratory work (10%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination.
2 Courseworks and work done in a lab.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks.
Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam.

Additional Notes:

Available to visiting and exchange students.

CSCM23 Designing-in Trust, Understanding and Negotiation

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr B Muller, Prof M Roggenbach, Dr AZ Wyner

Format:

Delivery Method: Lectures

Module Aims: This module explores state-of-the-art methods and concepts to assist responsible design and development of technology with the aim of creating reliable and trusted systems. The content of this module will be delivered by expert lecturers and practitioners in the areas of trusted computation, bias and explainability in automated decision making and decision support, ethical considerations for AI, argumentation and negotiation, as well as formal methods, such as verification of critical systems.

Module Content: - Data privacy in theory and practice
- Standards and practice of ethically-aligned design for autonomous and intelligent systems
- Notions of trust and trusted negotiations; argumentation
- Explainable AI; counterfactuals
- Formal methods and verification of system properties
- Law and regulation for AI

Intended Learning Outcomes: Students will learn to:
- Apply methods ensuring reliability, ethical standards, and legal compliance, as well as trust in technological systems
- Throughout the development process
- Appraise of the quality of data, including bias and provenance
- Design explainable decision processes
- Incorporate principles of data privacy
- Develop systems that achieve trust through transparency
- Incorporate formal methods into the development process to ensure safety and security.

Assessment:	Coursework 1 (30%) Examination 1 (70%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Coursework (Assessment level marking - PGTM): Essay (individual)
Examination, Assessment level marking - PGTM: Separate topics from each lecturer involved in teaching the module

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Individual written feedback for coursework component, e.g., annotated essays.

Failure Redemption: Resit examination.

Additional Notes:

Updated August 2023.

CSCM28 Security Vulnerabilities and Penetration Testing

Credits: 15 Session: 2023/24 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr JE Blanck

Format: 30 hours lectures and labs

Delivery Method: On-campus lectures and lab sessions.

Module Aims: The aim of this course is to examine methodological and practical aspects of cyber security threats and analysis techniques.

Module Content: Security threats and their causes.
Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection.
Countermeasures for attacks.
Security analysis tools and frameworks: including Kali Linux and Metasploit.
Shell code.
Legal and ethical issues of ethical hacking.
Social Engineering.
Methodologies for penetration testing.

Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures.
Students will be able to explain in detail a number of methodologies for security analysis of a system.
Students will have practical experience in recognising vulnerabilities and will be able to defend against them.
Students will be able to apply techniques of penetration testing to existing systems, and gain a critical awareness of the limits of these techniques.

Assessment:	Examination 1 (50%) Coursework 1 (10%) Coursework 2 (10%) Assignment 1 (4%) Assignment 2 (3%) Assignment 3 (3%) Assignment 4 (4%) Assignment 5 (3%) Assignment 6 (5%) Assignment 7 (4%) Assignment 8 (4%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination.
2 Courseworks and work done in a lab.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for coursework. Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam.

Additional Notes:

Available to visiting and exchange students.

CSCM29 Blockchain, Cryptocurrencies and Smart Contracts

Credits: 15 Session: 2023/24 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr AG Setzer

Format: 30 hours including presentation and consultation hours

Delivery Method: On-campus lectures and lab sessions.

Module Aims: This is a module on modern blockchain technology and its major applications. It will give an overview on the technological setup of major cryptocurrencies, and introduce the blockchain as a concept for determining the order of events in a distributed database. In addition, it will discuss the implementation of smart contracts and summarise the current state of the art of security issues in cryptocurrencies, blockchain technology, and smart contracts.

Module Content: Introduction to cryptocurrencies, blockchain technology and smart contracts
History of cryptocurrencies.
From the model of a bank to the Bitcoin model.
The Bitcoin client.
Transactions, keys, addresses, wallets.
The Bitcoin network.
Mining and consensus.
An overview over other cryptocurrencies.
History and Philosophy of Ethereum.
Smart contracts.
Smart contract development using Solidity.
Security of Smart Contracts.

Intended Learning Outcomes: Students will be able to

- explain blockchain technology and critically evaluate its current and future applicability,
-- explain the theoretical concepts behind cryptocurrencies and blockchain technology, and be able to critically reflect on issues surrounding their application, -
- explain the concepts behind smart contracts, be able to apply them in a lab environment, and critically evaluate their applicability as a technology,
- develop and document software related to the areas of cryptocurrencies, blockchain technology, and smart contracts.
-- apply blockchain technology to scenarios in a lab and critically evaluate its usability potential in the real world.

Assessment:	Examination 1 (70%)
	Coursework 1 (10%)
	Coursework 2 (10%)
	Laboratory work (10%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination, duration 2hrs.
Coursework 1: Java-based exercise (Java programming skills required)
Coursework 2: Solidity coursework
Laboratory Work: Practical Work

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks.
Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam and/or resubmit assignments as appropriate.

Additional Notes: Available to visiting and exchange students.

CSCM38 Advanced Topics: Artificial Intelligence and Cyber Security

Credits: 15 Session: 2023/24 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Prof SA Shaikh, Prof J Zhang

Format: 20 lectures, 5 x 1hr seminars, 3 x 2hr labs, 2 drop-in hours.

Delivery Method: On-campus lectures and lab sessions.

Module Aims: This module introduces students to the state-of-the-art methods and research topics of artificial intelligence,

cyber security, including quantum computing, data science, deep learning and reinforcement learning. The

inspiration behind these approaches will be discussed, along with their relative merits for application in cyber

security.

Module Content: 1. Advanced AI Topics: Deep Supervised Learning: Advanced Topics on CNNs, RNNs and GNNs.

2. Advanced AI Topics: Deep Unsupervised Learning: Advanced Topics on AE, Autoregression Models, Flow, GANs.

3. Data Security: Federated Learning, Differential Privacy in Learning.

4. Model Security: Adversarial Attack and Defense, Robustness Testing.

5. AI for Cybersecurity: Malicious Intrusion Detection etc

Intended Learning Outcomes: Student will be able
- to demonstrate a broad knowledge of the state-of-the-art concepts and techniques of artificial intelligence (AI) for cyber security,
- to appraise vulnerabilities and risks introduced by AI,
- to compare and contrast different analysis methods for cyber security problems,
- to carry out independent research on AI and data science topics related to cyber security.

They should further be able
 to transfer the knowledge to solve cyber security problems, from a computation, artificial intelligence and data science perspective.

Assessment:	Coursework 1 (50%) Coursework 2 (50%)
Resit Assessment:	Coursework reassessment instrument (100%)

Assessment Description: Coursework 1: This is a written essay of 2,500 words to be completed on an individual basis. The essay is a structured mix of analytical discussion and technical working around a case study, which requires individuals perform some background research, engaged with the case study materials provided, and perform critique and synthesis over a range of technical configurations. This component also requires engagement with lecture and seminar materials, which are designed to guide individuals on the threat analysis and risk assessment needed for the component case study.

Coursework 2: This is a written essay of 2,500 words to be completed on an individual basis. The essay is an in-depth and guided research effort, demonstrating the use of an organised literature search and methodology to perform a critical review of some of the state-of-the-art in a selection of topics relevant to the module. This research-led component asks for the individuals to engage in the lecture and practical sessions so that appropriate scientific and technical insights are drawn on the concepts explored, and also provide for effective commentary on the use of such concepts to address the problems posed in the module content.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Individual written feedback and cohort feedback

Failure Redemption: Resubmit coursework as appropriate.

Additional Notes: Available to visiting and exchange students

CSCM48 Web Application Development

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr SP Walton

Format: 18 hours lectures, 12 hours labs

Delivery Method: On-campus lectures and lab sessions.

Module Aims: The module will develop the principles and technologies used for building web-based systems. Practical experience of building web systems will be gained via laboratories and coursework. Existing high programming skill and experience is essential for this module.

Module Content: The history of web application development.
HTML and CSS: Introduction and Good Practices.
Web Application Design.
MVC driven web applications
Security and identity in web applications
Web development using Javascript and AJAX

Intended Learning Outcomes: Students will have a systematic understanding of the key aspects of current web programming principles and technologies.
Students will be able to plan and deliver a web application to a deadline.
Students will be able to create web applications following methodological good practice.
Students will be able to design secure web applications and evaluate their effectiveness.
Students will be able to design web applications which provide basic analytics for system administrators.

Assessment:	Coursework 1 (20%)
	Coursework 2 (10%)
	Coursework 3 (70%)
Resit Assessment:	Coursework reassessment instrument (100%)

Assessment Description: Coursework 1 and 2 - Code Review and code submission.

An important part of working in a software engineering organisation is code reviews. In this process engineers look at each other's code to spot bugs and ensure standards are being adhered to. You will submit a source file from your project to be reviews by another student and review another student's source file. You will be assessed both on your adherence to standards with your source code and the quality of your code review.

Coursework 3 - Implementation.

You will submit the implementation of a small web application. You will be asked to evaluate this by answering a series of questions referencing your implementation. This will assess both your knowledge of the theory and ability to apply that in practice.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Feedback during Presentation of work.
Outline solutions provided along with group and individual analytical feedback for courseworks.
Individual feedback on submissions from lecturer and/or demonstrators in laboratory sessions.

Failure Redemption: Resit examination and/or resubmit coursework(s) as appropriate

Additional Notes: Students taking this module must have good programming skills (i.e., be a competent programmer in any standard programming language) as this module requires significant programming ability.

Available to visiting and exchange students.

CSCM85 Modelling and Verification Techniques

Credits: 15 Session: 2023/24 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr U Berger

Format: 20 hours lectures;
2 x 3 practicals;
4 problem consultation hours.

Delivery Method: primarily on campus

Module Aims: This module will give an overview of the landscape and the state of the art of current modelling and verification techniques. One particular tool for software verification will be studied in depth. Students will gain hands-on experience in using that tool.

Module Content: Overview of techniques for formal verification.
Interactive theorem proving, automated theorem proving and model checking.
Introduction to one specific logic for modelling and verification.
Techniques for modelling of software using verification tools.
Practical verification of software examples.

Intended Learning Outcomes: The students will have
- gained an thorough overview of the landscape and the state of the art of current modelling and verification techniques
- acquired a deep understanding of one particular verification tool and know how to translate practical and mathematical problems into its notation
- obtained hands-on experience in practical verification.

Assessment:	Examination 1 (70%) Coursework 1 (15%) Laboratory work (15%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard format Computer Science exam (2 hours), and coursework:

Assignment 1: Mathematical and logical foundations of concurrent processes.
Assignment 2: Advanced modelling and verification in the process language CSP.
Lab: Modelling and verification in CSP using the process tools ProBE and FDR.

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks.
Examination feedback summarising strengths and weaknesses of the class.
Individual feedback on submissions from lecturer and/or demonstrators in laboratory sessions.

Failure Redemption: Resit examination and/or resubmit coursework(s) as appropriate

Additional Notes:

Available to visiting students

CSCM88 Network and Wireless Security

Credits: 15 Session: 2023/24 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr P Kumar

Format: 30 hours lectures and labs

Delivery Method: On campus lectures and labs.

Module Aims: Low cost networked computers add eyes and ears (or sensors) and arms, legs and voices (or actuators) to the Internet – called the Internet of Things (IoT) connected smart objects. Networking technologies play a critical role in almost all modern software-based systems, whether the fixed networks of computers, or the growing pervasive devices which have increasingly diverse profiles of network connectivity. As a result, they provide a potential vector for many forms of attack and are an ideal location for many threat mitigations and isolation technologies.

Module Content: Overview of Cryptography -- Basic encryption and decryption: terminology, substitution, stream, and block ciphers; characteristics of good ciphers. Symmetric and asymmetric encryption. Encryption algorithms: DES, RSA, AES, etc. Hashing.

Network fundamentals -- TCP/IP, SSL/TLS review, tools for network analysis, routing algorithms, threat modelling, network attachment protections: RADIUS, EAP, 802.1x, etc.

Network defense -- Form of firewalls, behaviours and design, and layered protections

Intrusion detection -- Techniques for detecting abnormal patterns of behaviours.

Mobile Network systems -- Security complexities introduced by mobility, security architecture and protocols.

Security in wireless sensor networks (WSN) -- WSN architectures and protocols, security threats, cryptographic primitives, key establishment and distribution, security of ZigBee WSNs, security of Industrial-IoT devices (as a case study), formal verification, and future trends.

Case Studies -- AKA (Authentication and Key Agreement): 4/5G security; IoT security – 6LowPAN and CoAP IETF standards.

Intended Learning Outcomes: 1) Students will have the ability to identify security vulnerabilities and their causes in modern networking infrastructures.
2) Students will be able to explain and apply techniques from networking protocols.
3) Students will be able to apply skills learned to designing and developing secure emerging wireless networks.
4) Students will be able to apply techniques to enhance the security of existing networks and gain a critical awareness of the limits of these techniques.

Assessment:	Examination 1 (70%)
	Coursework 1 (15%)
	Laboratory work (15%)
Resit Assessment:	Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination.
Laboratory Work: Project-based lab work.
Coursework 1: Practical network-based assignment

Moderation approach to main assessment: Moderation by sampling of the cohort

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks.
Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam.

Additional Notes:

Available to students on Specialist Master programmes.