OXFORD BROOKES UNIVERSITY

PROGRAMME SPECIFICATION

for the award of

MSc in Computer Science for Cyber Security

Managed by the Faculty of Technology, Design and Environment

delivered by School of Engineering Computing and Mathematics

Date approved:	2018
Applies to students commencing study in:	September 2021

RECORD OF UPDATES

Date amended*	Nature of amendment**	Reason for amendment**
July 2016	Transferred to new template	CMA Compliance
October 2016	Checked for errors and amended by Subject Coordinator and Programme Lead.	Subject specialist knowledge
November 2016	Checked by Faculty Quality Team	Following further CMA Compliance guidance
November 2018	Module list changed	Module list changed
September 2019	Double coded modules	System requirements
December 2020	Change of module codes acceptable (same modules but different codes)	Consolidation of module codes
December 2020	Removal of sandwich mode	Consolidation of delivery

SECTION 1: GENERAL INFORMATION

Awarding body:	Oxford Brookes University
Teaching institution and location:	Oxford Brookes University, Wheatley Campus
Language of study:	English
Final award:	MSc, PG Diploma, PG Certificate
Programme title:	Computer Science for Cyber Security
Interim exit awards and award titles available:	MSc Computer Science for Cyber Security Postgraduate Diploma Computer Science for Cyber Security Postgraduate Certificate Computer Science for Cyber Security
Brookes course code:	MSC-CYB PGD-CYB PGC-CYB
UCAS code:	P060038
JACS code:	I100
HECoS code:	100376
Mode of delivery:	Full-time (face to face/on-campus) Part-time (face to face/on-campus)
Mode/s and duration of study:	PG Cert Full time – minimum 1 semester, maximum 5 years PG Cert Part time – minimum 2 semesters, maximum 5 years PG Dip Full Time - minimum 2 semesters, maximum 5 years PG Dip Part Time - minimum 4 semesters, maximum 5 years MSc Full Time - minimum 1 year, maximum 5 years MSc Part Time - minimum 2 years, maximum 5 years
QAA subject benchmark statement/s which apply to the programme:	Computing http://www.qaa.ac.uk/en/Publications/Documents/SBS-Masters-degree-computing.pdf
Professional accreditation attached to the programme:	Provisional GCHQ
University Regulations:	The programme conforms to the University Regulations for the year of entry as published/archived at: http://www.brookes.ac.uk/regulations/

SECTION 2: WHY STUDY THIS PROGRAMME?

Many existing computer science professionals have only basic knowledge of cyber security. They lack the expertise and skills that are required to securely design and build the complex, highly dynamic systems and software used in the modern world. To be a proficient and professional practitioner in this area requires the ability to stay up to date with rapidly changing technologies and to have the competence to apply these technologies effectively. The industry needs graduates who are well versed in applying cyber security concepts to conventional computer science problems. Graduates need, not only to understand the fundamentals of cyber security but also to be able to apply them to the various technologies and systems that are used in a modern business context.

The Computer Science for Cyber Security programme holds provisional certification from GCHQ. The programme extends the knowledge gained in a first degree and teaches students the fundamental concepts needed to produce the secure systems needed for today. The programme explores key ideas in computer science from a cyber security perspective. The theory taught in lectures is reinforced in practicals, where students have the opportunity to use industry-standard tools and techniques, in our dedicated server and networking laboratories, which provide a safe space for students to practise both offensive and defensive security techniques.

The programme's emphasis on live projects, including group work modelled on industry-standard working patterns, gives students the opportunity to learn skills and concepts that are directly applicable to the workplace.

In addition to the award of MSc, the course is offered with the awards of Postgraduate Diploma and Postgraduate Certificate for those students who wish to learn a particular aspect of the discipline.

The aim of the MSc programme is to produce students who have learnt the fundamental principles of computer science and cyber security. In particular, students will have a comprehensive knowledge of the core aspects of networking, operating systems, secure programming, system development, cyber security and systems security auditing and testing. The students will have had the opportunity to use a wide range of enterprise software and hardware in our dedicated security laboratory. Students will also have had the opportunity to work in a professional manner, both individually and in teams, and will have had experience of a variety of roles commonly associated with designing and developing secure IT systems and software. Students will have produced reports which document their investigations in the style that would be expected if they were working in industry. In their dissertation, students will have carried out a more detailed design and implementation of an IT security system or have taken the opportunity to evaluate one of the emerging technologies in this area.

Students completing the Postgraduate Diploma programme will have learnt the fundamental principles of computer science and cyber security. In particular, students will have a comprehensive knowledge of the core aspects of operating systems, system development, cyber security and systems security auditing and testing. The students will have had the opportunity to use a wide range of enterprise software and hardware in our dedicated security laboratory. Students will also have had the opportunity to work in a professional manner, both individually and in teams, and will have had experience of a variety of roles commonly associated with designing and developing secure IT systems and software. Students will have produced reports which document their investigations in the style that would be expected if they were working in industry

Students completing Postgraduate Certificate programmes will have extended their knowledge in their chosen area of Computer Science and Cyber Security. Students will also have had the opportunity to work in a professional manner both individually and in teams. Students will have produced reports that document their investigations in the style that would be expected if they were working in industry.

Please refer to the following link to view the staff profiles within the Department of Computing and Communication Technologies:

http://cct.brookes.ac.uk/staff/index.html

SECTION 3: PROGRAMME LEARNING OUTCOMES

On successful completion of the programme, graduates will demonstrate the following Brookes Attributes:

3.1 ACADEMIC LITERACY

A01	Demonstrate a thorough understanding of the fundamentals of cyber security and its application in order to design and implement secure systems.
A02	Demonstrate a thorough understanding of fundamental networking and systems technologies and techniques for the creation and maintenance of secure IT systems.
A03	Critically evaluate information risk management and security issues of computer systems and software to create efficient and secure solutions for given real world problems that align to business needs.
A04	Critically appraise emerging technologies and techniques and identify and assess the potential benefits and risks for future systems.
A05	Create abstractions, from observed patterns encountered across the whole spectrum of real world problem domains, to facilitate the analysis and synthesis of appropriate solutions and to derive suitable meta level patterns.
A06	Apply appropriate methodologies to develop and implement IT infrastructure that will address the information requirements of organisations in order to meet business goals in a secure manner.
A07	Demonstrate a thorough understanding of legal and ethical frameworks in cyber security and their use and application in a business context.
A08	Conduct an investigation into a cyber security incident, summarise and report findings and create recommendations to reduce the risk of re-occurrence
A09	Demonstrate a thorough understanding of human factor issues in cyber security and utilise them in design, implementation, maintenance and use of IT systems and software to enhance security.

3.2 RESEARCH LITERACY

R01	Demonstrate self-direction and originality in planning and managing a research project and synthesise relevant research based materials in the organisation of the project.
R02	Critically analyse research based material and synthesise an independent perspective on the subject based on an evaluation of research techniques.
R03	Demonstrate a systematic understanding of knowledge of current problems and/or new insights, much of which is at or is informed by the forefront of computer science or relevant area of professional practice.
R04	Understand and participate in the process of peer review and publishing academic work.
R05	Analyse a complex security scenario, structure it, collect relevant information, consider options and recommend a course of action.

3.3 CRITICAL SELF-AWARENESS AND PERSONAL LITERACY

C01	Evaluate and reflect on the evolution of their strengths and weaknesses across the range of subject based competences involved in the domain.
C02	Participate in, and direct group activities, and apply self-awareness in recognising and evaluating the importance of teamwork, time management, communication, problem resolution and initiative.

C03	Create solutions to problems, acting autonomously, and make decisions in challenging situations in planning, implementing and delivering tasks in a given time scale.

3.4 DIGITAL AND INFORMATION LITERACY

D01	Demonstrate effective skills and practices necessary to become a confident, agile adopter of a range of technologies for personal, academic and professional use.
D02	Create a secure solution to a complex problem using existing appropriate software tools.
D03	Use appropriate technologies, such as online libraries and databases, to find, critically evaluate and utilise both non domain specific (e.g. standards, papers and reports) and domain specific (e.g. ISO standards, APIs and RFCs).
D04	Demonstrate proficiency in a range of modes of communication such as giving presentations to groups, writing reports and writing software documentation.

3.5 ACTIVE CITIZENSHIP

G01	Identify and analyse risk, reliability, legal, social, environmental, professional and ethical issues relevant to research and problem solving in the domain.
G02	Evaluate the impact of security considerations in the design, development and use of computer and communication systems in economic, political, cultural and social contexts in both national and international settings.
G03	Design and create software and IT solutions suitable for a global market with due regard to legal and ethical considerations of security and privacy.
G04	Critically evaluate software and systems in an ethical manner with due regard to legal and privacy issues.

SECTION 4: CURRICULUM CONTENT & STRUCTURE

4.1 PROGRAMME STRUCTURE AND REQUIREMENTS:

Requirements for an MSc (180 credits):

Code	Module Title	Credits	Level	Status	Coursework: Exam ratio
TEC7005	Research, Scholarship and Professional Skills	20	7	Compulsory	100% Coursework
SOFT7006	Secure Systems Architecture	20	7	Compulsory	50% Coursework:50% Exam
NEWT7013	Enterprise Networking	20	7	Compulsory	100% Coursework
NEWT7006	Malware Analysis	20	7	Compulsory	100% Coursework
NEWT7007	Operating Systems Security and Development	20	7	Compulsory	100% Coursework
NEWT7008	Secure Programming	20	7	Compulsory	50% Coursework:50% Exam
TECH7009	MSc Dissertation in Computer Science	60	7	Compulsory	100% Coursework
TECH7003	Independent Study II	20	7	Optional	100% Coursework

Requirements for Postgraduate Diploma (120 credits):

Code	Module Title	Credits	Level	Status	Coursework: Exam ratio
TECH7005	Research, Scholarship and Professional Skills in Cyber Security	20	7	Optional	100% Coursework
SOFT7006	Secure Systems Architecture	20	7	Compulsory	50% Coursework:50% Exam
NEWT7013	Enterprise Networking	20	7	Optional	100% Coursework
NEWT7006	Malware Analysis	20	7	Compulsory	100% Coursework
NEWT7007	Operating Systems Security and Development	20	7	Compulsory	100% Coursework
NEWT7008	Secure Programming	20	7	Optional	50% Coursework:50% Exam
TECH7009	MSc Dissertation in Computer Science for Cyber Security	60	7	Optional	100% Coursework
TECH7003	Independent Study II	20	7	Optional	100% Coursework

Requirements for Postgraduate Certificate (60 credits):

Code	Module Title	Credits	Level	Status	Coursework: Exam ratio
TECH7005	Research, Scholarship and Professional Skills in Cyber Security	20	7	Optional	100% Coursework
SOFT7006	Secure Systems Architecture	20	7	Optional	50% Coursework:50% Exam
NEWT7013	Enterprise Networking	20	7	Optional	100% Coursework
NEWT7006	Malware Analysis	20	7	Optional	100% Coursework
NEWT7007	Operating Systems Security and Development	20	7	Optional	100% Coursework
NEWT7008	Secure Programming	20	7	Optional	50% Coursework:50% Exam
TECH7009	MSc Dissertation in Computer Science for Cyber Security	60	7	Optional	100% Coursework
TECH7003	Independent Study II	20	7	Optional	100% Coursework

4.2 PROGRESSION AND AWARD REQUIREMENTS

The following modules are acceptable for the subject. Students must pass all modules marked 'Compulsory', as well as meeting the university rules for postgraduate programmes.

Students studying for an MSc must complete at least 180 credits worth of modules.

Students studying for a Postgraduate Diploma must complete at least 120 credits worth of modules.

Students studying for a Postgraduate Certificate must complete at least 60 credits worth of modules.

Students who choose to progress from a Postgraduate Certificate to a Postgraduate Diploma may be required to take additional credits, over the 120 normally required for a Postgraduate Diploma in order to ensure that they have completed all the compulsory modules for the Postgraduate Diploma.

4.3 PROFESSIONAL REQUIREMENTS

None.

SECTION 5: TEACHING AND ASSESSMENT

Students will attend lectures to acquire the knowledge and understanding of the key concepts. This includes lectures on Research and Scholarship Methods.

Practical work is an important part of this programme. The practical elements of the course are designed to reinforce the theoretical learning, put it in a real world context and gain experience of industry standard equipment and software. Students will acquire experience on which to reflect and develop professional expertise. In most modules, the coursework associated with the practical work forms at least half of the total assessment.

Several modules will include an element of team working, enabling students to collaborate with their peers thus developing an awareness of their own abilities, as reflected by feedback from others. Teamwork will also be used to assess the students' acquisition of personal and inter-personal skills, so important for this degree, and equally important for most career paths in the industry.

Modules have 10 learning hours per module credit. For the 20 credit taught modules, this is 200 learning hours, for the dissertation, this is 600 learning hours. Learning hours are broken down in contact and non-contact hours. For taught modules this normally consist of 4 hours contact per week, divided into 2 hours of lecture and 2 hours of supervised practical/tutorial work. Exceptions to this are –

- TECH7003/P00014 Independent Study 2 – This module is guided learning and will run in a variety of modes. It is only available to students in exceptional circumstances.
- PCYRSM Research, Scholarship and Professional Skills in Cyber Security – This module has 2-4 hours of lecture per week, plus seminars as needed.

Students on the dissertation will arrange supervision sessions with their supervisor(s) as needed. It is expected that each student will contact their supervisor(s) at least once every 2 weeks during the dissertation period.

Students will be expected to study additional hours outside of the scheduled contact time and this may include time in the network labs.

The mix of coursework to exam will vary depending on the modules chosen and is given for each module in section 4.1. For an MSc, for the compulsory modules this will be – dissertation, PCYRSM, NEWT7006/P00501, NEWT7007/P00502 – 100% coursework; SOFT7006/P00410, NEWT7008/P00503 – 50% coursework:50% exam; P00552 - 35% Coursework:15% Practical Exam:50% Written Exam.

Academic Literacy will be assessed through a mixture of examination and coursework, testing the students' ability to explain key concepts and to apply them to practical problem solving. The first semester focuses on basic principles, and this is built on in the second semester, where more complex systems and network concepts are introduced.

Research Literacy is taught through the Research, Scholarship and Professional Skills in Cyber Security module and through literature review and analysis assignments in other modules. This includes the instruction and practice of producing reports, to a professional standard, and this is assessed. These skills are then further applied, and practised, in the compulsory dissertation module where it is also assessed.

Critical Self-awareness and Personal Literacy will be supported through the use of a reflective component included in a variety of courseworks. Students will be asked to reflect on their performance and identify areas of strength and weakness. They will be encouraged to actively address any weaknesses, identified in semester 1, during semester 2, and then further reflect on whether satisfactory improvement has been made.

Digital and Information Literacy is fundamental to the academic content of this degree and will be a distinguishing feature of graduates from the programme. In particular, students are expected to make extensive use of industry standards in both computer science and cyber security. A significant part of the assessment, for the modules, will be based on the student's ability to use these tools and report the resultant analysis in a professional manner.

Effective use of ICT in teaching is also a key part of the department's learning and teaching strategy. The department actively uses Moodle for electronic access, communication and feedback and makes extensive use of ebooks, online videos, podcasts and other electronic resources.

IT systems are now ubiquitous in modern life. This has economic and social benefits but, to continue to be successful, the industry should behave responsibly in terms of ethics, sustainability and the environment and to operate within a regulatory framework. These active citizenship issues, and considerations, are discussed within each module and are assessed either in the coursework or in the examination.

The management of risk is now an important skill for all graduates. This programme creates an awareness of the meaning and significance of risk. Guidelines for risk management, in the Research and Scholarship Methods module, and specific instances and examples are raised throughout the programme, relevant to the module topic. It is assessed in either the examination or coursework of each module.

By paying due regard to the Oxford Brookes University's Assessment Compact, the assessments on this programme have been designed to develop the learning of technical skills, shaped by the underlying theory and requirements of the industry. Assessment does not present students with a set of hurdles, but rather guides them through the staged acquisition of a complex set of professional skills so that, by the time they graduate, they are ready to play an effective role in their chosen career. Feedback on the assessment tasks will be provided in a timely manner, emphasising the achievement of the learning outcomes of the modules and the programme. Students will be encouraged to relate the assessment tasks, with professional activities, and to relate their achievements with professional standards. Where appropriate, self and peer assessment will be used to encourage students to involve themselves in their own professional development.

On this programme, the assessment compact ideals are realised as follows. Semester 1 is designed to introduce the fundamental concepts in advanced computer science and in cyber security. Early coursework on NEWT7013/P00506 and NEWT7012/P00505 ensures that students have the opportunity to quickly assess their competencies with core ideas in the domain and their approach to research. This is built on throughout the semester on these two modules. Although SOFT7006/P00410 only has 1 coursework assessment point at the end of the module, the practical sessions on that module explores the concepts introduced in the lecture and gives the students opportunities to evaluate their learning of those concepts. Also included in SOFT7006/P00410 is a reflective assessment where students are required to reflect on their learning to date and how that has evolved and changed.

In week 0 of semester 2, students will meet with their subject co-ordinator to discuss their semester 1 performance and to develop an individual learning plan to build on their semester 1 achievements and to address any shortcomings or deficiencies. Semester 2 itself builds on the foundations laid in semester 1 and introduces more complex concepts, ideas and techniques in cyber security. This is introduced in a staged manner with the early teaching, learning and assessment covering the key concepts which are then build upon in the later courseworks. Early teaching and learning in the semester 2 modules will stress the link between that material and the semester 1 modules. Early assessment in the semester 2 modules will require the students to reflect on this progression. Assessment due in at the end of semester 2 modules will require the students to reflect back on their learning on that module and the relationships between the materials covered on all their modules to date.

Semester 3 is the dissertation and forms the capstone of their work. Students are supported through out the dissertation with a strong emphasis on research and project planning in the early part of the dissertation. As the student progresses, they are guided to become more independent learners and will take ownership of the dissertation project, including the requisite project management. By the completion of the dissertation, the students will be fully independent learners capable of managing a substantial project, and will, in the form of their short paper, have been involved with the academic peer review process and will have potentially contributed to the wider scientific community.

The department is committed to inclusivity and diversity in its teaching. By the very nature of the discipline, virtually all of our teaching material is available in an accessible format and, where possible, we follow best practice guidelines and make our electronic material available before the lectures. We also use electronic references, and eBooks, to further enhance accessibility. Inclusivity and diversity is also embedded in what we teach. All new students have a lecture on inclusivity and diversity as part of their induction, and important inclusivity and diversity topics, such as the need for accessibility and internationalisation, and how to achieve them, are taught on a variety of modules throughout the degree.

SECTION 6: ADMISSION TO THE PROGRAMME

6.1 ENTRY REQUIREMENTS

For September 2017;

The university's general entry requirements are:

http://www.brookes.ac.uk/studying-at-brookes/how-to-apply/entry-requirements/postgraduate-courses/

You should normally hold a first degree, equivalent to at least a British lower second-class bachelor's degree, in an Electronic Engineering, Telecommunications, Computer Science or a related Engineering or Computing degree.

Applicants whose first degree is not in these areas, but who have worked in a related industry, and have obtained good relevant experience and programming skills can also be considered.

If your first language is not English you will require a minimum IELTS score of 6.0 with 6.0 in all components. Also see the university's standard English requirements:

http://www.brookes.ac.uk/international/applying-to-arriving/how-to-apply/english-language-requirements/

SECTION 7: PREPARATION FOR EMPLOYMENT

According to research conducted by e-skills UK and the National Sector Skills Council for IT and Telecommunications, the IT professional workforce, in the UK, has almost doubled in the last 20 years, and is likely to continue growing at 5-8 times the average employment growth for the coming decade.

It is no longer acceptable to develop, and deploy, IT systems and software without significant consideration of security issues. Indeed, the UK Government's National Security Council identifies cyber-attack as one of the 4 highest priority risks for the UK. In particular, they highlight the lack of computer science graduates, with the necessary skills in cyber security, as a serious concern for both government and industry, with demand far outstripping supply.

Graduates therefore require a comprehensive conceptual and technical understanding of the core fundamentals in computer science and cyber security, coupled with the development of methods of analysis, interpretation and synthesis of knowledge and concepts, for application to complex problem solving, project management and to maintain currency for the future.

A key feature of the programme is its standards-based, industrially relevant approach. The use of industry standard tools, in a hands-on environment, in our security laboratories, provides students with real world experience of industry standard tools and techniques.

The programme provides graduates with a thorough foundation of computer science and cyber security, equipping them with the skills necessary for a career within industrial, government and commercial environments including such roles as software developer, IT systems manager, network architect, IT security manager, as well as design and consultancy roles.

Many modules use guest speakers from industry to illustrate the practical application of the module material. Potential employers are keen to talk to a wide spectrum of students and they will discuss the nature of their industry as well as how the students might contribute to the companies.

The Department maintains close links with the University's Careers Office. Themed 'mini' careers fairs are organised by the Department, with technology being a common theme. Students are encouraged to use the facilities offered which include CV workshops, practice interviews and assessment-centre activities.

An Industrial Liaison Board is run within the Department, with senior employees of regional and representative organisations as members. The board is consulted on major initiatives within the Department, including programme revalidations, possible research partnerships, future trends and directions and the feasibility of new course offerings.

An alumni organisation has recently been formed in the Department. The aim of this organisation is to invite ex-students, who are now in a variety of technical and managerial roles, to network with each other and with our current students. It is anticipated that this organisation will be of great benefit to students starting out in their careers, as well as for more senior alumni looking to use the skills and expertise of the staff and students in the Department.

Research centres, within the Department, are actively involved with Knowledge Transfer Partnerships and other links with employer organisations. One of the spin-offs from these activities is the on-campus presence of industrial-based experts, in fields closely related to our degree offerings.

At the University level, there are dedicated support services both for specific groups of students, such as Oxford Brookes International and the Disability Advisory Service, and for all students such as Upgrade, the university's study skills development/support service.