UNIVERSITY of BRADFORD

Faculty of Engineering and Informatics

Department of Computer Science

Programme Specification

Programme title: MSc Cyber Security

Academic Year:	2019/20
Degree Awarding Body:	University of Bradford
Partner(s), delivery organisation or support provider (if appropriate):	
Final and interim award(s):	[Framework for Higher Education Qualifications (FHEQ) level 7] MSc Postgraduate Diploma Postgraduate Certificate
Programme accredited by (if appropriate):	British Computer Society (BCS)
Programme duration:	1 year full time, 2 years part-time
QAA Subject benchmark statement(s):	Master's Degree in Computing
Date last confirmed and/or minor modification approved by Faculty Board	March 2019

Please note: This programme specification has been published in advance of the academic year to which it applies. Every effort has been made to ensure that the information is accurate at the time of publication, but changes may occur given the interval between publishing and commencement of teaching. Any change which impacts the terms and conditions of an applicant's offer will be communicated to them. Upon commencement of the programme, students will receive further detail about their course and any minor changes will be discussed and/or communicated at this point.

Introduction

The programme was originally introduced in 2004. The programme as a whole has been significantly revised to enhance its contents and ultimately the skills of all students graduating. This development process has taken a number of years and as such has included discussion and feedback from a number of academics, students, alumni, professionals and external examiners. This programme has been delivered each year since 2004.

The main goal of this MSc Cyber Security programme is to prepare professionally trained graduates for industry. In this respect, detailed discussions have taken place, initially with industry professionals, who along with all other stakeholders

have had a major input into shaping the revised programme. The key motivation for the current programme curriculum is to ensure that all graduates have studied relevant security disciplines that reflected the aims of the GCHQ National Security Programme whilst adhering to the curriculum framework within the University of Bradford. In effect, it is considered imperative that students will have an in depth understanding of the issues faced by modern organisations. The programme is designed to offer graduates the opportunity to develop a deeper understanding of cyber security as a discipline. The focus within this programme on the principles, technologies and practices of cyber security helps students to gain the appropriate skills for future PhD studies and research careers as well as to become competent practitioners.

The programme comprises particular developments in security with a firm base in academic research and also offers the opportunity for students to study selected topics in advanced computer science. The programme includes the opportunity to enhance industry relevant skills with study in ISO27001 Lead Implementer and Ethical Hacking. These skill areas were highlighted by past alumni and industry practitioners for inclusion in the programme. Within this programme therefore, students have the opportunity to gain additional qualifications in: Certified ISO/IEC 27001 Lead Implementer; and CEH v8 Ethical Hacking.

This programme meets a continued growing demand for specialists in this area by offering a way for individuals in current employment with relevant industry experience as well as recent graduates to study and enhance and develop their skills. The MSc Cyber Security programme will therefore draw graduates wishing to enhance their undergraduate studies in computing with advanced study of security to equip them for senior positions with responsibility for the IT technical and management based security of an organisation. In addition, the programme admissions criterion encourages those with relevant industry skills to specialise in cyber security or refine and develop their existing expertise. The School of Electrical Engineering and Computer Science (SEECS) has for many years successfully taught a range of programmes at undergraduate and postgraduate level. This programme draws upon the successful research expertise of the SEECS from within the Faculty of Engineering and Informatics in the University in addition to that within the Interdisciplinary Research Centre (IRC) in Cyber Security. This IRC has members from within Peace Studies, Engineering, Electrical Engineering, Computer Science, Mathematics, Telecommunications, Management, Law, Social Science and Phycology. This broad base of expertise and research is a fantastic resource for the continued development of the programme in cyber security.

Students get exposure to industry throughout their programme as this is embedded in a number of ways. Our Industry Advisory Board (IAB), with a membership comprised of industry representatives from both regional and national companies, meets twice a year to review our existing provision and to propose improvements to our courses. Throughout the academic year industrial speakers deliver invited talks that inform and inspire our students about current and future developments within their disciplines. In addition, industry qualifications such as ISO27001 Lead Implementer and CEH v8 Ethical Hacking are integral to the programme design.

Student societies with links to professional bodies afford further opportunities for our students to engage with industry, such as Pi Soc as the first ever BCS Student Chapter, and our ACM student chapter. These societies are encouraged and supported by the School to participate in industry led activities such as programming competitions, data dives and extra-curricular visits.

Our teaching is informed by industry in several ways. Staff undertaking KTP projects, national and EU funded research projects and consultancy work embed new knowledge and concepts into their teaching materials and curriculum planning, based on the research and development work they conduct.

Programme Aims

The MSc programme in Cyber Security is intended to:

- Respond to current academic challenges provided by increasing reliance on computers and networks for core business activity and to meet commercial needs for employees who are able to understand and think strategically about future developments in this area.
- Provide a high academic quality of service to students, covering both theoretical and practical aspects of computing, networking and cyber security.
- Enable students to equip themselves with knowledge, skills and understanding, at an advanced level within the chosen field of study.

Programme Learning Outcomes

To be eligible for the award of Postgraduate Certificate at FHEQ level 7, students will be able to:

LO1. Demonstrate an advanced understanding and application of some of the theories, principles and techniques applicable in the field of Cyber Security;
LO2. Demonstrate a systematic understanding and critical awareness of secure; systems within an organisation and the technical, legal and business issues involved;
LO3. Demonstrate a systematic understanding and critical awareness of the nature of a computer related crime and the people and organisations involved therein;
LO4. Demonstrate an advanced understanding of, and ability to apply concepts and principles underlying cryptographic primitives and protocols;
LO5. Demonstrate a comprehensive and critical understanding of techniques specific to the field of computer security;

Additionally, to be eligible for the award of Postgraduate Diploma at FHEQ level 7, students will be able to:

LO6. Critically analyse, model, construct and evaluate specific types of networks and be able to effectively implement a reliable and effective security protocol;
LO7. Select, adapt and apply the underlying technologies of secure systems;
LO8. Mastery of the practical and theoretical concepts of computer science, current and emerging trends in technology

Additionally, to be eligible for the award of Degree of Master at FHEQ level 7, students will be able to:

LO9. Select, design, plan and manage a self-directed and managed research-informed project;

LO10. Demonstrate a critical awareness of current and possible future opportunities and problems in; Internet, Computer and System Security evaluating current developments and trends.

On successful completion of the MSc Cyber Security students will be able to achieve mastery of the principles and applications of network, computer and systems security through:

Systematic **Knowledge and Understanding** and a critical awareness at advanced level, of core computing, networking and security subjects including security technologies, detailed understanding of the implications and issues relating to secure applications; recognition of the influence of the cyber world on secure system design and evaluation, and application development for firewalls, authentication, encryption, certificates and security protocols.

Discipline Specific Skills, showing: originality in the application of knowledge, together with a practical understanding of how established techniques of research and enquiry in security and cyber technologies are used to create and interpret knowledge in the discipline; the ability to design, implement, and evaluate secure systems; development of critical understanding of regulatory and practical issues relating to cyber security:

Personal and Transferable Skills necessary for employment requiring: the exercise of initiative and personal responsibility; decision-making in complex and unpredictable situations; and the independent learning ability required for continuing professional development.

Curriculum

The MSc Cyber Security covers a range of specialist topics, leading to the qualification of a Master's degree with the option to study for additional industry qualifications. Typically, a taught full-time Master's programme lasts for twelve months of full-time study (twenty four months part time). The programme has two stages: the taught programmes stage which takes place during the first two semesters (or four semesters for the part-time route), and the project/dissertation stage. The taught programmes stage is organised on a modular basis.

The programme is structured in terms of Core modules. The relevance of the programme’s content to the stated teaching aims and objectives is based on core computer science and informatics topics as well as modules on relevant cyber security in relationship to secure implementation of systems, and their application in practice. Students will have opportunity to enhance Personal Transferable skills principally through participation in and taking responsibility for a major individual project.

The programme has modules in semester one and two providing grounding and advanced study of the field. The final semester allows students the opportunity to develop, through sustained major project work, advanced knowledge and understanding of cyber security.

Postgraduate Certificate

Module Code	Module Title	Type	Credits	Level	Semester
COS7035-B	Business Systems Security	C	20	7	1
COS7024-B	Networks and Protocols	C	20	7	1

COS7047-B	Advanced Cryptography	C	20	7	1

Students will be eligible to exit with the award of Postgraduate Certificate if they have successfully completed 60 credits and achieved the award learning outcomes.

Postgraduate Diploma

Module Code	Module Title	Type	Credits	Level	Semester
COS7023-B	Internet Security and Protocols	C	20	7	2
COS7030-B	ISO27000 Framework (ISMS)	C	20	7	2
COS7029-B	Ethical Hacking	C	20	7	2

Students will be eligible to exit with the award of Postgraduate Diploma if they have successfully completed 120 credits and achieved the award learning outcomes.

Degree of Master

Module Code	Module Title	Type	Credits	Level	Semester
COS7004-E	Dissertation	C	60	7	3

Students will be eligible for the award of Degree of Master if they have successfully completed 180 credits and achieved the award learning outcomes.

The curriculum may change, subject to the University's programme approval, monitoring and review procedures.

Learning and Teaching Strategy

The programme includes innovative and active learning methods. Throughout the programme, we make use of case studies so that students can apply their theoretical understanding to real-world issues. In this way, abstract concepts are brought to life through practical activities. We also use methods associated with the "flipped classroom" where content is outside the classroom leaving more time and space for activities and active learning within tutorial and lecture sessions.

In addition to the standard technology enhanced learning approaches, we embed technologies to deliver key concepts in an interactive environment that strongly links theory with practical skills. For example, we link remotely with industry experts to deliver interactive sessions for developing student's pen-testing skills.

Research active staff are involved in curriculum development based on their research activities, exposing students to the very latest and future developments within their field of expertise. We integrate knowledge and experience from Industrial partners through both our Industry Advisory Board and research projects through case studies, lab based activities and invited talks, ensuring that research findings are at the heart of our curriculum.

The programme offers a curriculum with core elements in Cyber Security. Dissertation work further enriches the opportunities students have to take control of their own learning. A range of teaching and learning methods is employed including lectures, tutorials, laboratory work and directed private study. Each 20-credit module on the programme requires students to commit 200 hours of study. Some of these hours will be formally timetabled - lectures, laboratories, seminars, tutorials and workshops whilst others will involve students carrying out private study.

Four workshop sessions act as a springboard for consideration and integration of Legal Social Ethical and Professional (LSEPI) issues into the project work from its commencement. All students progressing onto the dissertation are required to attend these workshops. As part of the workshop series, seminar sessions will take place to introduce the concepts and wider context of LSEPI practices within the Computing discipline (e.g. analysis skills, the research process, dissertation outlines and managing projects, data protection, computer misuse, ethics etc.). The seminars define relevant terms and the implications for professional practice within Computing. These are followed by a tutorial session with a case study scenario for groups of students, and the members of staff supervising dissertations, to discuss and debate the various aspects of LSEPI practice that would impact upon the scenario and the possible decisions and hypothetical outcomes. The tutorial concludes with a plenary to discuss the wide variety of issues and viewpoints from the groups and the implications for their dissertation work.

To ensure these topics are developed within a students' dissertation period, these initial workshops will be strengthened through the requirement for students to discuss these issues with their supervisor on a one to one basis. In addition, students will be required to complete an Ethical Approval Form with the aim of highlighting any potential ethical and legal implications of the work proposed.

Assessment Strategy

Assessment for this programme is designed to develop skills in the area of cyber security in addition to more generic professional transferable skills such as team working, communication, leadership and decision making. The combination of group work, individual submissions, examinations, theoretical work and lab based

exercises helps develop skills that are essential in industry. Alongside gaining an MSc Cyber Security, students have the opportunity to gain additional qualifications in ISO/IEC 27001 Lead Implementer and CEHv8 Ethical Hacking if they undergo additional assessment.

All of our staff have achieved, or are working towards, Fellowship of the Higher Education Academy. As part of our commitment to Excellence in Learning and Teaching, we conduct research into innovative and effective teaching methods. For example, assessment for projects was enhanced by incorporating regular formative and summative feedback opportunities to enhance the final outcomes.

Assessment Regulations

This Programme conforms to the standard University Regulations which are available at the following link:

http://www.bradford.ac.uk/aqpo/ordinances-and-regulations/

Admission Requirements

The University welcomes applications from all potential students and most important in the decision to offer a place is our assessment of a candidate's potential to benefit from their studies and of their ability to succeed on this particular programme. Consideration of applications will be based on a combination of formal academic qualifications and other relevant experience.

The standard entry requirements for the programme are as follows:

Entry requirements: Typically 2:2 or above. Applications are welcome from students with non-standard qualifications or mature students (those over 21 years of age on entry) with significant relevant experience.

Recognition of Prior Learning

If applicants have prior certificated learning or professional experience which may be equivalent to parts of this programme, the University has procedures to evaluate and recognise this learning in order to provide applicants with exemptions from specified modules or parts of the programme.

Minor Modification Schedule

Version Number	Brief description of Modification	Date of Approval (Faculty Board)
4	Changes to incorporate core modules and remove options as per GCHQ feedback	
5	Updates for Academic Portfolio Review in February 2016	December 2015
6	Modification to curriculum structure	March 2019