MSc in Computer and Information Security

Primary Purpose:
Course management, monitoring and quality assurance.

Secondary Purpose:
Detailed information for students, staff and employers. Current students should refer to the related Course Handbook for further detail.

Disclaimer:
The University of Portsmouth has checked the information given in this Programme Specification and believes it to be correct. We will endeavour to deliver the course in keeping with this Programme Specification but reserve the right to change the content, timetabling and administration of the course whilst maintaining equivalent academic standards and quality.

Contents

Programme Specification

1. Named Awards

MSc Computer and Information Security

2. Course Code (and UCAS Code if applicable)

C2386F and C2386P

3. Awarding Body

University of Portsmouth

4. Teaching Institution

University of Portsmouth

5. Accrediting Body

None at present.

6. QAA Benchmark Groups

Computing.

7. Document Control Information

Release 6.0, July 2016

8. Effective Session

2016/2017

9. Author

Dr Benjamin Aziz

10. Faculty

Faculty of Technology

11. Department

School of Computing

12. Educational Aims

The general aim of the MSc in Computer and Information Security programme is to equip its students with scientific and professional experience in the field of computer and information security. More specifically, the course aims at:

- Providing a challenging, stimulating and self-rewarding study environment.
- Developing a range of key skills in areas covered by the course by means of opportunities provided in the study units
- Accommodating student needs in relation to maximising their career potential and professional responsibility by enabling them to develop knowledge, understanding and skills in their chosen subject area related to computer and information security

- Developing research skills and techniques to enable students to undertake Doctoral or other research work in Computer and Information Security or other relevant areas

13. Reference Points

This section sets out the reference points that have been consulted in the development of the course and which demonstrate that the programme has currency and relevance within the academic, professional and employer communities:

- University of Portsmouth Curricula Framework Document (July 2012)
- The scholarship and research expertise of academic members of staff
- QAA Code of Practice for the Assurance of Academic Quality and Standards in Higher Education
- National Qualifications Framework
- Subject Benchmark Statements (SBS).

14. Learning Outcomes

The following sections highlight the various skills that the students can develop throughout the course. These are divided into knowledge and understanding skills, cognitive skills, practical skills and transferable skills.

A. Knowledge and Understanding of:

A.1 Security models, threats and techniques as applied to distributed systems
A.2 Wireless network and Web security and vulnerabilities
A.3 Software engineering methodologies for eliciting system design requirements and constraints
A.4 Formal languages (e.g. the "B" refinement language) for the modelling, preparation and validation of system specifications
A.5 Risk matrices and risk mitigation strategies
A.6 Evaluation of classification technique in relation to Cyber-security attacks
A.7 Science of digital forensic and the investigative process as applied to computer systems and digital information
A.8 Theory and application of cryptography and cryptanalysis to achieving secure systems
A.9 Project planning, evaluation and maintenance

Learning and Teaching Strategies and Methods

Knowledge and understanding will be gained through lectures, tutorials, practical work, group work and project work, with lectures at a proportion of roughly 50% of the course exposure time and the rest occupying the remaining 50%. Extensive use will be made of case studies (often using external speakers) where theoretical principles and practical implications will be systematically and critically discussed.

Assessment

Assessment will be both formative and summative, consisting of a combination of continuous assessment, dissertations, coursework assignments, project work and formal examinations.

B. Cognitive (Intellectual or Thinking) Skills, be able to:

B1. Explain the various approaches and techniques for developing secure distributed systems
B2. Critically analyse and evaluate security properties and threats in distributed systems
B3. Use formal methods in modelling, analysing and validating system properties and requirements
B4. Explain the different stages of the risk management process and be able to choose the appropriate technique in every stage
B5. Critically evaluate the applicability of various digital forensic techniques to criminal scenarios
B6. Evaluate and apply cryptographic functions and information in securing distributed systems
B7.Evaluate and apply security solutions to a real world problem by means of a project-based solution

Learning and Teaching Strategies and Methods

Intellectual skills are developed throughout class sessions, seminars and discussion groups, whereas the use of case studies, worked examples and journal papers helps prepare students to think critically and challenge conventional technologies and models in the relevant areas of the course.

Assessment

Assessment of the levels of cognitive learning will be through the use of exams as well as coursework assignments, dissertations and reports.

C. Practical (Professional or Subject) Skills, be able to:

C1. Select and apply security mechanisms, such as access control policies and authentication protocols, in improving the security level of a computer system
C2. Use software tools for writing and reasoning about security policies
C3. Use software tools effectively in order to analyse and develop requirements and formal specifications for constructing secure systems
C4. Use data mining software to analyse a range of security-related datasets, making an appropriate choice of algorithm in each case
C5. Use a range of digital forensic tools in the context of a digital investigation
C6. Apply cryptographic operations for various purposes related to the security of a system
C7. Manage computer engineering and study projects using appropriate tools and techniques

Learning and Teaching Strategies and Methods

Practical skills will be developed throughout class and laboratory sessions as well as seminars and discussion groups/workshops and supervised project work. The use of case studies, worked examples, reports and journal papers will help prepare the students to think critically about their professional role and develop innovation based on existing literature and technologies.

Assessment

Assessment will be through examinations, presentations, dissertations and reports for assessing practical, professional and subject specific skills. This could be for example through practical investigations of digital devices, and simulated experience of giving expert witness evidence in the case of forensic assessments of practical skills.

D. Transferable (Graduate and Employability) Skills, be able to:

D1. Communicate effectively through writing and presenting their work
D2. Read and understand complex documentation related to the technical material in the course
D3. Use of scientific evidence based methods in the solution of problems
D4. Selectively use IT skills in the development of projects material
D5. Apply problem-solving ideas in the development of innovative solution
D6. Ability to work effectively in multi-disciplinary teams to achieve objectives
D7. Ability to achieve successfully the aims and objectives of a Masters project.

Learning and Teaching Strategies and Methods

Transferable skills are developed by individual and group presentations, case studies giving examples of best practice in security engineering problem solving and teamwork to demonstrate the integration of security engineering and other disciplines.

Assessment

Use is made of examinations, presentations, dissertations and group and individual reports, where approximately half the work involves group activities and the remainder is individual. This helps strengthen transferable skills of students such as learning how to communicate effectively their ideas with given deadlines, similar to real world scenarios.

15. Course Structure, Progression and Award Requirements

- The course will comprise four core units, each weighted at 30 credits equivalent to 300 notional hours of study. In addition to these, the course will also include a project unit weighted at 60 credits equivalent to 600 notional hours.
- There are two modes of study: Full time and part time. The full time mode completes in 12 months and the part time mode in 36 months.
- The degree of MSc in Computer and Information Security will be awarded based on the successful completion of 180 credits (four core units and the project).
- On successful completion of 60 credits, a student may exit the programme with the award of a Postgraduate Certificate in Computer and Information Security. On successful completion of 120 credits, a student may exit with the award of a Postgraduate Diploma in Computer and Information Security. Standard University rules apply. The Regulations must be consulted for a full description of exit awards.

16. Employability Statement

Computer and Information security remains at the forefront of the issues related to the global digital economy and national defence. The course aims at equipping graduates with necessary technical knowledge and skills to fulfil the needs of industry for security professionals in areas related to systems and network security, requirements engineering, risk management and threat analysis, and modelling and analysis of security and digital forensics, through providing several career paths based on knowledge and expertise gained in this course. Such career roles include security engineer, security architect, R&D researcher in security-related projects and forensic analyst. The course will also strengthen research skills by means of the M.Sc. projects undertaken to prepare research minded graduates to pursue an academic and industry research career in collaboration with the collaborative ties maintained by the Network and Computer Security research group in the School of Computing with various scientific and industrial sectors, both at the national and the EU levels.

17. Support for Student Learning

- The Course is managed by a Course Leader.
- Extensive induction programme introduces the student to the University and their course.
- Each student has a personal tutor, responsible for pastoral support and guidance.
- University support services include careers, financial advice, housing, counselling etc.
- The Academic Skills Unit (ASK).
- The Additional Support and Disability Advice Centre (ASDAC).
- Excellent library facilities.
- The University of Portsmouth has consistently been awarded an excellent rating for student support and guidance in a number of Quality Assurance Agency inspections.
- Student course and unit handbooks provide information about the course structure and University regulations etc.
- Feedback is provided for all assessments.
- Personal Development Planning (PDP) for all awards.
- English for Academic Purposes (EAP).

18. Admissions Criteria

A. Academic Admissions Criteria

Standard University rules apply and this will normally mean that candidates are in possession of an honours degree with at least a classification of 2.2 and in a relevant discipline. All other qualification or experience presented must be forwarded to the Head of School for a decision on acceptance. Evidence of competence in the use of the English Language must be demonstrated, typically by an IELTS score of

6.0 where candidate's first language is not English.

B. Disability

The University makes no distinction in its admissions policy with regard to disability and will endeavour to make all reasonable adjustments in order to make it possible for students to study at Portsmouth on a course of their choice.

19. Evaluation and Enhancement of Standards and Quality in Learning and Teaching

A. Mechanisms for Review and Evaluation

- Course Leader's Annual Standards and Quality Evaluative Review.
- Head of Department's Annual Standards and Quality Evaluative Review.
- Unit and Course Level student feedback considered at Board of Studies.
- Unit Assessment Board consideration of student performance for each programme.
- Annual Standards and Quality Reports to Board of Studies, including consideration of Subject and Award External Examiner Reports.
- Periodic Programme Review.
- Student Representatives and Student/Staff Consultative Committees.
- National Student Survey.
- Staff Performance and Development Review.
- Peer Review and Development Framework.
- Faculty Learning and Teaching Committee.

B. Responsibilities for Monitoring and Evaluation

- Unit Co-ordinators for unit content and delivery.
- Course Leader for day-to-day running of course.
- Board of Studies with overall responsibilities for operation and content of course.
- Head of Department.
- Associate Dean (Academic).
- Associate Dean (Students).
- Quality Assurance Committee.
- Unit, Award and Progression Board of Examiners.

C. Mechanisms for Gaining Student Feedback

- Student Representation on Board of Studies.
- Student Staff Consultative Committees.
- Unit and Course level student feedback questionnaires.
- University participates in external student surveys, eg National Student Survey (NSS), Postgraduate Research Experience Survey (PRES) and International Student Barometer (ISB).

D. Staff Development Priorities

- Academic staff members undertake activities related to research, scholarship, teaching and learning and student support and guidance.
- Annual staff performance and development reviews match development to needs.
- Managers undertake a variety of management development programmes.
- All academic staff encouraged to seek Higher Education Academy membership.
- Academic staff new to teaching required to undertake Initial Professional Development Programme (iPROF).

- Support Staff are encouraged to attend short courses in areas such as minute taking, and specific IT packages.

20. Assessment Strategy

Level 7 students should show a professional approach to work and research, and demonstrate that they have: developed independence of thought; a high level of intellectual rigour and consistency; excellent academic/ intellectual skills; considerable creativity and originality; and excellent research skills.

A variety of assessment styles are used in different units. Practical skills are assessed in coursework and supervised work sessions. In these, students need to demonstrate the ability to reflect on the work, not simply report it. The assessments are designed to allow appraisal of skill, and for the students to demonstrate a wider contextual understanding of what they are doing. Ethical considerations are often directly assessed in units. Supervised Work Sessions provide an opportunity to demonstrate effective professional skills, working in teams (characteristic of many areas of the computing industry), and communicating and reporting. The Project is the opportunity for students to draw together skills and knowledge acquired from different taught units, and use them to develop or research an appropriate and secure technical solution.

21. Assessment Regulations

Standard university rules apply (see Assessment and Regulations).

22. Role of Externals

Subject External Examiners who will:

- oversee unit assessment and usually attend Unit Assessment Boards;
- review unit assessment strategy;
- sample assessment artefacts;
- present report to Unit Assessment Boards.

Award External Examiners (usually also a Subject External Examiner) who will:

- oversee and attend Award/Progression Boards;
- scrutinise and endorse the outcomes of assessment;
- ensure that the standard of the award is maintained at a level comparable with that of similar awards elsewhere in the United Kingdom.

23. Indicators of Standards and Quality

A. Professional Accreditation/Recognition

None at present.

B. Periodic Programme Review (or equivalent)

A Periodic Programme Review was conducted in March 2015. The curriculum was confirmed as being fit for purpose and the annual monitoring and review processes were confirmed as effective.

C. Quality Assurance Agency

QAA Higher Education Review, March 2015, judgements about standards and quality meet UK expectations (*for full report see Higher Education Review of the University of Portsmouth, March 2015*[1]).

[1] www.qaa.ac.uk/en/ReviewsAndReports/Documents/University%20of%20Portsmouth/University-of-Portsmouth-HER-15.pdf

D. Others

None.

24. Other Sources of Information

Other sources of information may be found in

- Course Approval Document.
- Student Handbook.
- University of Portsmouth Curricula Framework.
- University of Portsmouth Undergraduate Prospectus.
- Assessment Regulations.
- University of Portsmouth (http://www.port.ac.uk/) and School of Computing (http://www.port.ac.uk/comp) websites.

Unit Assessment Map

UNITS						COURSEWORK				EXAMINATION			
Level	Name	Code	Credit	Delivery	Core/ Option	Total %	Type of Artefact	Duration/ Length	Weighting %	Total %	Open/ Closed	Duration (hrs)	Weighting %
7	Computer Security (CSEC)	P22240	30	Year	C	100	Coursework	3000 words	40	100	Closed	3 hours	60
7	Formal Approaches to Software Development (FASDEV)	P22435	30	Year	C	100	SWS involving a presentation Essay	20 min 2,500 words	25 25	100	Closed	2	50
7	Risk Management and Data Analytics (RIMADA)	P24351	30	Year	C	100	Coursework Coursework	3000 equiv. 3000 equiv.	50 50				
7	Computer Forensic Investigation & Cryptography (COMFIC)	P22434	30	Year	C	100	Essay SWS1 SWS2	4,000 words Practical Report/Presentation within both SWSs	40 30 30				
7	Masters Engineering Project (PJE60)	U22244	60	Non-standard Campus	SCO	100	Dissertation Research and Professionalism Presentation	Report, 10-12K words Essay, 3000 words Oral presentation (20 minutes)	80 15 5				
7	Masters Study Project (PJS60)	U22445	60	Non-standard Campus	SCO	100	Dissertation Research and Professionalism Presentation	Report, 10-12K words Essay, 3k words Oral presentation (20 minutes)	80 15 5				

Unit Learning Outcomes Map[2]

UNITS					LEARNING OUTCOMES																										
Name	Code	Credit	Delivery	Core/ Option	A1	A2	A3	A4	A5	A6	A7	A8	A9	B1	B2	B3	B4	B5	B6	B7	C1	C2	C3	C4	C5	C6	C7	D1	D2	D3	D4	D5	D6	D7
Computer Security(CSEC)	P22240	30	Year	C	x	x								x	x						x	x						x	x	x	x	x	x	
Formal Approaches to Software Development (FASDEV)	P22435	30	Year	C			x	x								x							x					x	x	x	x	x	x	
Risk Management and Data Analytics (RIMADA)	P24351	30	Year	C					x	x							x							x				x	x	x	x	x	x	
Computer Forensic Investigation & Cryptography (COMFIC)	P22434	30	Year	C							x	x						x	x						x	x		x	x	x	x	x	x	
Masters Engineering Project (PJE60)	U22244	60	Non-standard Campus	SCO									x							x							x							x
Masters Study Project (PJS60)	U22245	60	Non-standard Campus	SCO									x							x							x							x

[2] A = Knowledge and Understanding; B = Cognitive (Intellectual) Skills; C = Practical (Subject Specific) Skills; D = Transferable Skills