Programme Specification

MSc Cyber Security (2018-19)

This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

Awarding Institution	University of Southampton
Teaching Institution	University of Southampton
Mode of Study	Full-time
Duration in years	1
Accreditation details	British Computer Society (BCS)
Final award	Master of Science (MSc)
Name of award	Cyber Security
Interim Exit awards	Postgraduate Certificate in Higher Education
	Postgraduate Diploma in Higher Education
FHEQ level of final award	Level 7
UCAS code	N/A
Programme code	5471
QAA Subject Benchmark or other external reference	Master's Degree Characteristics 2016, Master's Degrees In Computing 2011
Programme Lead	Julian Rathke (jr1a06)

Programme Overview

Brief outline of the programme

In recent years, cyber security has emerged to be a topic of critical importance to commercial and academic organisations, to governments, and to their citizens.

The International Telecommunications Union (ITU-T) has defined cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and the assets of organisations and users”, adding that “cyber security strives to ensure the attainment and maintenance of the security properties of the assets of organisations and users against relevant security risks in the cyber environment.” [http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx]

The UK government, amongst others, has recognised the shortage of skilled practitioners of cyber security, in particular those who have a well-rounded, multi-disciplinary view of the subject area, embracing not only technical matters but also aspects of risk management, criminology, and legal and social factors.

This MSc aims to deliver such a multi-disciplinary cyber security programme, primarily targeted as a broadening qualification for computer science graduates (or a closely related subject plus significant computing experience), and thus a bridge between an undergraduate degree and a career in cyber security. The modules which comprise this Masters degree cover state of the art techniques, technologies, and supporting tools, and expose students to their applications in meeting emerging cyber security challenges.

The programme is part of an emerging multi-pathway cyber security offering at Southampton that we are building in collaboration with other departments including Management, Law and Criminology.

The programme is delivered through collaboration between experts in departments who are participants in the GCHQ/EPSRC Academic Centre of Excellence for Cyber Security Research (ACE-CSR) at Southampton [https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research]. Together, the Centre and the MSc form a symbiotic relationship by making our expertise available and applying the research and knowledge shared by our external industry contacts. As part of our growing cyber security activities, we are also exploring the creation of a new Cyber Security Academy, to be based at Southampton and involving a number of high profile businesses in the area.

A key feature of the programme is the individual summer project that, subject to agreement, we expect you to undertake in collaboration with an industry partner as part of the supervision team. The Project Preparation module, which is compulsory in the second semester, will help ensure you have met and held discussions with your project supervision team to identify appropriate research question(s), that you have then conducted an appropriate literature review, developed the necessary skills and formed an appropriate project plan in advance of the commencement of your summer project. Where an industrial partner is not available, which may depend on your country of origin, you would undertake a project supervised by staff whose interests lie within those of the Southampton ACE-CSR.

NCSC/GCHQ Certification

This is 1 of only 25 cyber security MSc programmes in the UK to be awarded Certification by the National Cyber Security Centre, part of GCHQ [https://www.ncsc.gov.uk/information/ncsc-certified-degrees].

This Certification is subject to students taking the six compulsory modules (excluding Project Preparation): COMP6224, COMP6230, COMP6236, CRIM6008, COMP3217 and ELEC6242.

Your contact hours will vary depending on your module/option choices. Full information about contact hours is provided in individual module profiles.

Learning and teaching

Learning and teaching methods are explained in the following sections covering programme learning outcomes.

Assessment

Assessment methods are explained in the following sections covering programme learning outcomes.

Special Features of the programme

Southampton is recognised in the UK by the EPSRC and by GCHQ for its expertise in cyber security through the award of its Academic Centre of Excellence in Cyber Security Research (ACE-CSR) status. Our specialist modules are taught by staff who are involved in leading edge research. Students are therefore exposed to the most up to date thinking, current research problems, and state of the art techniques, technologies and tools.

Please note: As a research-led University, we undertake a continuous review of our programmes to ensure quality enhancement and to manage our resources. As a result, this programme may be revised during a student's period

of registration; however, any revision will be balanced against the requirement that the student should receive the educational service expected. Please read our Disclaimer to see why, when and how changes may be made to a student's programme.

Programmes and major changes to programmes are approved through the University's programme validation process which is described in the University's Quality handbook.

Educational Aims of the Programme

The aims of the programme are to:

a) Equip you with an advanced knowledge of multi-disciplinary cyber security principles, and to enable you to recognise the importance of a multi-disciplinary approach to addressing cyber security.
b) Offer you the opportunity to study in a leading, interdisciplinary and research-intensive environment.
c) Develop your transferable research skills and interdisciplinary knowledge for a wide range of information and technology, research and policy careers.
d) Stimulate your interest in the application of cyber security by using a variety of teaching and learning methods and engaging with a wide range of cyber security perspectives.
e) Develop your ability to assess and manage both security and risk in a corporate environment.
f) Give you a broad yet advanced understanding of the social and human factors as they apply to criminology and cyber crime.
g) Develop and enhance your ability to identify research question(s) and conduct experimental or theoretical research, and to present the findings of such research in a clear, professional manner.
h) Expose you to a range of cyber security frameworks, standards and best practices that you will have the opportunity to demonstrate in applied scenarios.
i) Give you a “hands on” perspective on applying cyber security principles by undertaking a significant individual project, where possible with an industrial partner as part of the supervisory team.

Programme Learning Outcomes

Knowledge and Understanding

On successful completion of this programme you will have knowledge and understanding of:

A1. Key concepts of cyber security, including social, organisational and technological aspects of cyber security, their relationship, and the importance of a multi-disciplinary approach to handling cyber security;

A2. The range of disciplines, research methods and theoretical approaches required to analyse, critique, develop cyber security practices, and the range of state of the art techniques, frameworks, technologies and tools used to apply those practices;

A3. Current and emerging hot topics, challenges and research questions for cyber security;

A4. The application of multi-disciplinary cyber security principles and practices to a project in an industrial and/or research-led environment;

A5. Professional codes of practice, and legal, social, cultural and ethical issues related to cyber security, and an awareness of their societal and environmental impact.

Teaching and Learning Methods

Most modules primarily consist of a combination of lectures, small group teaching, practical work, directed reading and coursework assignments. You will also be set individual and (in some cases) group problem-based or design exercises, and will be expected to deliver presentations on your work to your peers. You are also expected to develop the skills necessary to undertake self-directed reading and, as part of your project preparation, conduct literature searches and surveys. One-on-one or small group tutorials can support full-class lectures, when required.
At the end of the taught part of the course you will undertake an individual project either in conjunction with an industrial partner (preferred) or with experts in Southampton's ACE-CSR. Small group teaching, including all practical work, and the individual project accommodate different learning styles. Invited guests from industry will give expert seminars on specific topics.

Assessment Methods

Testing of the knowledge base is through a combination of unseen written examinations and assessed coursework in the form of problem solving exercises, laboratory/exercise reports with literature review components, design exercises, and individual and small-group projects.

Subject Specific Intellectual and Research Skills

On successful completion of this programme you will be able to:

B1. Describe a variety of cyber security threats and perspectives; you will develop a broad understanding of the cyber threat landscape, both in terms of recent emergent issues and those issues and persistent threats which recur over time, and understand the roles and influences of governments, commercial and other organisations, citizens and criminals in cyber security affairs;

B2. Acquire and assess different ways of thinking and problem solving within and across disciplinary boundaries, including applying principles of criminology to appreciate the organisations and key stake holders in the business of preventing, controlling and policing cyber crime;

B3. Describe best practices in implementing secure systems, be able to appraise and analyse electronic and software systems for security hazards, and be aware of general principles and strategies that can be applied to such systems to make them more robust to attack;

B4. Analyse, evaluate and manage risk and security in a corporate environment, and understand the appropriate application of cyber security frameworks and best practices, including information security and risk management and operational security management, to a variety of cyber security scenarios.

B5. Find, read, understand and explain literature related to advanced and specialised areas of cyber security, including scientific publications, industrial documentation, standards, ethical, legal and environmental guidance, and be able to formulate an appropriately scoped cyber security research project from interpretation and analysis of that literature.

Teaching and Learning Methods

Most modules consist of a combination of lectures, small group teaching, and computer-based practical work, directed reading and coursework assignments, which can include a literature review.
The Project Preparation module and the Individual Project itself concern the formulation of a research

project. Small group teaching, including all practical work, and the individual project accommodate different learning styles. One-on-one or small group tutorials can support full-class lectures, when required.

Assessment Methods

Testing of the subject specific intellectual and research skills is through a combination of unseen written examinations and assessed coursework in the form of problem solving exercises, laboratory reports with literature review components, design exercises, and individual and small-group projects.
The Project Preparation module and the dissertation from the MSc Project include a significant literature survey and peer review, and have assessment criteria related specifically to these skills.
The Project dissertation is centrally focussed on applying cyber security principles in an industrial (through an industrial partner) or research-led (through the ACE-CSR) setting.

Transferable and Generic Skills

On successful completion of this programme you will be able to:

C1. Use a range of sources, both conventional and electronic, to locate relevant information, and critically appraise that information;

C2. Communicate effectively, and present specialist information in different written and verbal formats, tailored to a variety of audiences;

C3. Work effectively in a small group as a member of a team, managing you own contribution and the overall task;

C4. Work independently on a significant individual project, and understand the necessary steps to define and execute the project, managing time and risk in an effective manner;

C5. Recognise legal and ethical issues of concern to business, professional bodies, and society, including but not limited to information and cyber security, and follow appropriate guidelines to address these issues.

Teaching and Learning Methods

A number of courses have a significant coursework element. This can range from design work through to essays and presentations resulting from directed reading. The individual project includes independent research, project management and report writing.
C1-C3: Most modules include at least one of the following methods: small group teaching, practical work, directed reading and coursework assignments with a literature review component. The Project Preparation module includes project management and the delivery of a project plan via a presentation. Small group teaching, including all practical work, and the individual project accommodate different learning styles.
C4: The individual project includes independent research and report writing.
C5: Legal, ethical and professional issues are covered in the compulsory taught modules.

Assessment Methods

Coursework is generally assessed through written reports. The individual project is assessed by a dissertation of up to 15,000 words. The Project Preparation module is assessed via a literature review, as well as written and presentation versions of the project plan.

Subject Specific Practical Skills

On successful completion of this programme you will be able to:

D1. Use specialist software and analysis tools, and be able to evaluate, analyse and critique the security characteristics of software, and of networked systems and devices, including performing penetration and vulnerability testing.

Teaching and Learning Methods

Some modules include a level of practical work or exercises, for example involving use of specialised tools for software or systems analysis, or the application of specific frameworks to a given scenario.

Assessment Methods

Assessment is based on coursework in the form of written reports or essays, or reporting on the results of undertaking systems analysis and/or implementation, and also the MSc dissertation.

Programme Structure

The programme structure table is below:

Information about pre and co-requisites is included in individual module profiles.

Part I

Typical course content

The programme consists of eight taught modules, each worth 7.5 ECTS credit points (15 CATS) and an individual research project worth 30 ECTS credit points (60 CATS). Six compulsory modules cover core material for cyber security. Another compulsory module prepares you for your individual research project. One optional module can be selected

according to your interests. The total programme represents 90 ECTS (180 CATS) credit points.

Programme details

The programme runs over three semesters. The first semester consists of three compulsory modules and one optional module. The second semester consists of four compulsory modules. Following the first two semesters of the taught component of the programme, the students will undertake a research project which will be assessed by a degree dissertation.

For COMP6246 (Machine Learning Technologies) students should be comfortable with basic linear algebra and the fundamental principles of Calculus. With the approval of the programme leader, students with prior knowledge of linear algebra (including matrix operations), Calculus (including partial differentiation), probability and statistics can take COMP6245 (Foundations of Machine Learning) instead of COMP6246.

Most modules are shared with our Master of Engineering programmes in Computer Science and the other specialist MSc programmes we run, or with related MSc programmes that Southampton offers in other disciplines, specifically in Criminology, Web Science and Management. It should be noted that it may not be possible to run some optional modules if the number of students registered on the module is very small. It should also be noted that optional module choice can be restricted by the University Timetable, which varies from year to year: some optional modules may clash with other optional or compulsory modules. Please be aware that many modules are shared between different cohorts; the class size depends on cohort size, which varies from year to year.

Examinations are held at the end of Semester 1 (January) and at the end of Semester 2 (May/June). Students who have successfully completed 30 ECTS (60 CATS) or 60 ECTS (120 CATS) at the level of the award may exit with a Postgraduate Certificate or Postgraduate Diploma, respectively.

The following is the normal pattern of study for a full-time student, completing the programme within 12 calendar months.

Semester 1:
Four modules, including three compulsory modules and one optional module. Examinations are held in January.

Semester 2:
Four compulsory modules. Examinations are held in May/June.

Summer/Semester 3:
You will undertake a research project lasting 3 to 4 months, which is assessed by a 15,000 word dissertation.

The programme structure, including the optional modules, is summarised below:

====
SEMESTER 1 - select one optional module

COMP6224 - compulsory
COMP6230 - compulsory
COMP6236 - compulsory
COMP6204 - optional
COMP6242 - optional
COMP6246 - optional
CRIM6007 - optional

SEMESTER 2

ELEC6211 - compulsory
COMP3217 - compulsory
ELEC6242 - compulsory
CRIM6008 - compulsory

SUMMER

COMP6200 - core
====

Module information

The first semester contains three compulsory modules and offers a choice from four optional modules. The Foundations of Cyber Security module lays before you the broad, multi-disciplinary nature of cyber security, describing the landscape and, at a relatively high level, the relevant issues. Network and Web Based Security grounds many of these principles in their implementation, with a bias towards technical implementation, but in the context of recognised security frameworks. The module on Software Security looks at threats and hazards for software systems, best practices in implementing secure software, and techniques to analyse software, including the principles of reverse engineering.

The first semester optional module Machine Learning Technologies is available for students interested in applying data-driven analytical techniques to a variety of data sets. Students should be comfortable with basic linear algebra and the fundamental principles of Calculus. The optional Software Project Management and Development module prepares you for undertaking large software projects. Finally, you have the option of taking the Criminal Behaviour module, which introduces the social and human factors behind criminal behaviour, and may prove of interest to students wanting some focus on criminal theory.

The second semester has four compulsory modules. The first, Project Preparation, lays the foundation for your summer project, by giving you the necessary skills to plan and execute an appropriate project that is, where possible, negotiated with an industrial partner and two internal supervisors (usually from different disciplines). Cyber Crime, Insecurity and the Dark Web, covers the subject of the organisations and key stakeholders involved in the business of preventing, controlling and policing cyber crime. The Security of Cyber Physical Systems module equips students with the necessary skills and experience to understand, and attempt to counter, the principal threats to data and electronic system security. This module requires some familiarity with the C programming language. The Cryptography module gives a broad introduction into the subject of cryptography as it applies to electronic and computer systems. This module has quite significant mathematical content.

The summer period sees you undertake your Individual Project, which is a significant piece of experimental and/or research work. It is expected that where possible your MSc Project will involve an industrial partner. This would most likely mean that you would visit the industrial site as part of your work, though the amount of time spent on site may vary depending on the project. It is thus necessary to evaluate the viability of such placements during the Project Preparation module in Semester 2. Where an industrial partner is not available, which may be related to your country of origin, you would undertake a multi-disciplinary project within the University, most likely with experts from within our ACE-CSR.

Part I Compulsory

Code	Module Title	ECTS	Type
ELEC6242	Cryptography	7.5	Compulsory
CRIM6008	Cyber Crime, Insecurity and the Dark Web (Cyber Security)	7.5	Compulsory
COMP6224	Foundations of Cyber Security	7.5	Compulsory
COMP6230	Network and Web Based Security	7.5	Compulsory
ELEC6211	Project Preparation	7.5	Compulsory

COMP3217	Security of Cyber Physical Systems	7.5	Compulsory
COMP6236	Software Security	7.5	Compulsory

Part I Core

Code	Module Title	ECTS	Type
COMP6200	MSc Project	30	Core

Part I Optional

Select the equivalent of one full semester 1 module (7.5 ECTS/15 CATS) from the following:

Code	Module Title	ECTS	Type
COMP6246	Machine Learning Technologies (MSc)	7.5	Optional
COMP6242	Secure Software Development	7.5	Optional
CRIM6007	Criminal Behaviour - Applied Perspectives (Cyber Security)	7.5	Optional
COMP6204	Software Project Management and Development	7.5	Optional

Progression Requirements

The programme will follow the University's regulations for ***Progression, Determination and Classification of Results: Undergraduate and Integrated Masters Programmes*** or the University's regulations for ***Progression, Determination and Classification of Results: Standalone Masters Programmes*** as set out in the General Academic Regulations in the University Calendar: http://www.calendar.soton.ac.uk/sectionIV/sectIV-index.html

Support for student learning

There are facilities and services to support your learning some of which are accessible to students across the University and some of which will be geared more particularly to students in your particular Faculty or discipline area.

The University provides:

- library resources, including e-books, on-line journals and databases, which are comprehensive and up-to-date; together with assistance from Library staff to enable you to make the best use of these resources
- high speed access to online electronic learning resources on the Internet from dedicated PC Workstations onsite and from your own devices; laptops, smartphones and tablet PCs via the Eduroam wireless network. There is a wide range of application software available from the Student Public Workstations.
- computer accounts which will connect you to a number of learning technologies for example, the Blackboard virtual learning environment (which facilitates online learning and access to specific learning resources)
- standard ICT tools such as Email, secure filestore and calendars.

- access to key information through the MySouthampton Student Mobile Portal which delivers timetables, Module information, Locations, Tutor details, Library account, bus timetables etc. while you are on the move.
- IT support through a comprehensive website, telephone and online ticketed support and a dedicated helpdesk in the Hartley Library.
- Enabling Services offering support services and resources via a triage model to access crisis management, mental health support and counselling. Support includes daily Drop In at Highfield campus at 13.00 – 15.00 (Monday, Wednesday and Friday out of term-time) or via on-line chat on weekdays from 14.00 – 16.00. Arrangements can also be made for meetings via Skype.
- assessment and support (including specialist IT support) facilities if you have a disability, long term health problem or Specific Learning Difficulty (e.g. dyslexia).
- the Student Services Centre (SSC) to assist you with a range of general enquiries including financial matters, accommodation, exams, graduation, student visas, ID cards
- Career and Employability services, advising on job search, applications, interviews, paid work, volunteering and internship opportunities and getting the most out of your extra-curricular activities alongside your degree programme when writing your CV
- Other support that includes health services (GPs), chaplaincy (for all faiths) and 'out of hours' support for students in Halls and in the local community, (18.00-08.00)
- A Centre for Language Study, providing assistance in the development of English language and study skills for non-native speakers.

The Students' Union provides
- an academic student representation system, consisting of Course Representatives, Academic Presidents, Faculty Officers and the Vice-President Education; SUSU provides training and support for all these representatives, whose role is to represent students' views to the University.
- opportunities for extracurricular activities and volunteering
- an Advice Centre offering free and confidential advice including support if you need to make an academic appeal
- Support for student peer-to-peer groups, such as Nightline.

Associated with your programme you will be able to access:

· The tutorial system – you will have a personal tutor whom you can meet on request for advice on your programme and choice of options, or for pastoral support
· The ECS Student Advisory Team who provide additional pastoral support
· ECS computer workstations, with a range of manuals and books
· Specialist project laboratories
· Personal email account and web access, including use of on-line collaboration tools
· Helpdesk (programming advisory)
· Post-graduate demonstrators who provide additional support for your design projects
· A web-site for each taught module, typically with teaching materials

Methods for evaluating the quality of teaching and learning

You will have the opportunity to have your say on the quality of the programme in the following ways:

· Completing student evaluation questionnaires for each module of the programme.
· Acting as a student representative on various committees, e.g. Staff: Student Liaison Committees, Faculty Programmes Committee OR providing comments to your student representative to feed back on your behalf.
· Serving as a student representative on Faculty Scrutiny Groups for programme validation.
· Taking part in programme validation meetings by joining a panel of students to meet with the Faculty Scrutiny Group.

The ways in which the quality of your programme is checked, both inside and outside the University, are:

· Regular module and programme reports which are monitored by the Faculty.
· Programme validation, normally every five years.
· External examiners, who produce an annual report.
· Professional body accreditation/inspection.
· A national evaluation of research – which is relevant since our research activity contributes directly to the

quality of your learning experience.

- Higher Education Review by the Quality Assurance Agency.

Further details on the University's quality assurance processes are given in the *Quality Handbook.*

Career Opportunities

By offering a multi-disciplinary qualification we believe graduates of the programme will be very well placed to pursue careers in cyber security, particularly in private or government organisations where having a broader view of the problem space (rather than purely a technical view) will be advantageous.

There is also a very strong market for cyber security consultancy, and thus a growing number of consultancy organisations seeking graduates who understand cyber from a variety of perspectives.

The programme may also be well suited to people in mid career who are considering moving into cyber security as a change in career path, subject to having an appropriate grounding in computer science.

Alternatively, the MSc will form a solid platform for a research career or PhD in cyber security.

Graduates from our MSc programmes in ECS are employed worldwide in development and consultancy roles in a number of leading companies at the forefront of information technology; and some have gone on to doctoral study and University careers, while others have been involved in IT start-ups. ECS runs a dedicated careers hub which is affiliated with over 100 renowned companies like IBM, ARM, Microsoft Research, Imagination Technologies, Nvidia, Samsung and Google to name a few. Visit our careers hub4 for more information.

External Examiner(s) for the programme

Name: Dr Emil Lupu - Imperial College London

Students must not contact External Examiner(s) directly, and external examiners have been advised to refer any such communications back to the University. Students should raise any general queries about the assessment and examination process for the programme with their Course Representative, for consideration through Staff: Student Liaison Committee in the first instance, and Student representatives on Staff: Student Liaison Committees will have the opportunity to consider external examiners' reports as part of the University's quality assurance process.

External examiners do not have a direct role in determining results for individual students, and students wishing to discuss their own performance in assessment should contact their Personal Academic Tutor in the first instance.

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided. More detailed information can be found in the programme handbook.

Appendix 1:

Students are responsible for meeting the cost of essential textbooks, and of producing such essays, assignments, laboratory reports and dissertations as are required to fulfil the academic requirements for each programme of study. In addition to this, students registered for this programme also have to pay for:

Additional Costs

Type	Details
Stationery	You will be expected to provide your own day-to-day stationary items, e.g. pens, pencils, notebooks, etc). Any specialist stationery items will be specified under the Additional Costs tab of the relevant module profile.
Textbooks	Where a module specifies core texts these should generally be available on the reserve list in the library. However due to demand, students may prefer to buy their own copies. These can be purchased from any source. Some modules suggest reading texts as optional background reading. The library may hold copies of such texts, or alternatively you may wish to purchase your own copies. Although not essential reading, you may benefit from the additional reading materials for the module.
Approved Calculators	Candidates may use calculators in the examination room only as specified by the University and as permitted by the rubric of individual examination papers. The University approved models are Casio FX-570 and Casio FX-85GT Plus. These may be purchased from any source and no longer need to carry the University logo.
Printing and Photocopying Costs	In the majority of cases, coursework such as essays; projects; dissertations is likely to be submitted on line. However, there are some items where it is not possible to submit on line and students will be asked to provide a printed copy.

In some cases you'll be able to choose modules (which may have different costs associated with that module) which will change the overall cost of a programme to you. Details of such costs will be listed in the Module Profile. Please also ensure you read the section on additional costs in the University's Fees, Charges and Expenses Regulations in the University Calendar available at www.calendar.soton.ac.uk.