PROGRAMME SPECIFICATION – POSTGRADUATE PROGRAMME

KEY FACTS

Programme name	Cyber Security
Award	MSc
School	Mathematics, Computer Science and Engineering
Department or equivalent	Department of Computer Science
Programme code	PSCYSE
Type of study	Full Time
Total UK credits	180
Total ECTS	90

PROGRAMME SUMMARY

The MSc in Cyber Security will prepare you for a successful career in the various roles directly and indirectly connected to the world of computer, network and information security. It will develop your specialist analytical, operational and development skills in both technical and socio-technical areas of cyber security.

This course covers core areas of masters' level computer science, such as research methods and scientific presentation and analysis skills. It will enable you to specialise in some aspects of the area of cyber security and engage with researchers to develop your scientific knowledge and skills. The programme offers students to acquire knowledge in the sociotechnical aspects of security, (such as cyber-crime and sociotechnical risk), and in more traditional technical aspects (such as digital forensics and data analytics).

The course is designed for those who wish to extend their capability for an accelerated early career in cyber security and have completed a first degree in a computing subject (e.g. computer science, business computing) or a numerate subject (e.g. applied mathematics, engineering, physics) if that covered a significant computing component.

This course primarily objective is to give students practical experience with a shared Coursework (Cyber Security Challenge) that extends among all the security specific modules. With real-life scenarios and using metasploit tool this Coursework ensures hands-on experience in testing and analysing computing systems. This course is also subject to accreditation by GCHQ.

The programme provides a range of modules which include 15, 30 and 60 credit modules at masters' level. The programme provides you with a choice of exit routes.

POSTGRADUATE CERTIFICATE IN CYBER SECURITY. The first exit point is the Postgraduate Certificate in Cyber Security which you are able to achieve through successful completion of 4 out of 6 taught core security modules (Cryptography, Information Security Fundamentals, Network Security, Security Audit and Certification, Digital Forensics and Cyber Crime and Sociotechnical Risk). Those completing these modules will gain a fundamental understanding of Cyber Security role in today's computing environment and be able to apply basic security techniques and methods

appropriate in a security preservation process. Students will be able after completion of this stage to identify secure systems and their potential vulnerabilities. They will be able to evaluate designs for Cyber Security systems using a variety of techniques.

The assessments you undertake to achieve this qualification will focus on activities that you need to undertake either as part of your role or to support you in developing your professional practice.

The postgraduate certificate will enable you to develop confidence in your knowledge and skills in a career in Cyber Security.

POSTGRADUATE DIPLOMA IN CYBER SECURITY. A Postgraduate Diploma in Cyber Security may be achieved if you have successfully met the requirements of either of the Postgraduate Certificate awards and then successfully complete Research Methods and Professional Issues and one elective or two additional 15 credit elective modules.

For all of you completing the Postgraduate Diploma in Cyber Security in addition to the above you will gain basic research skills and deepen your understanding of more advanced theory in Cyber Security which are applied to innovative and complex technology. You will gain a knowledge for sociotechnical aspects not commonly considered in Cyber Security and apply specialist skills in assessing reliability. You will choose one elective module to explore some areas further to broaden your expertise and skills.

The assessments you undertake to achieve this qualification will again on activities that you need to undertake either as part of your role or to support you in developing your professional practice you wish to implement or examine further.

The postgraduate diploma will provide you with an extended repertoire of skills needed as you develop into an experienced professional and introduce you to the broader theories and techniques related to Cyber Security.

MSc IN CYBER SECURITY. For the MSc, you must in addition to achieving the requirements for one of the Postgraduate Diploma awards - complete successfully the Dissertation module INM363.

For all of you completing the MSc in Cyber Security in addition to the above you will participate in a Cyber Security Challenge, which is distributed between two semesters and examines the practical activities of the core modules.

The assessment for the project module is in the form of a traditional dissertation reporting your work.

The MSc will provide an opportunity to explore an aspect of Cyber Security in depth through the literature and empirical evidence and make recommendations to improve and develop Cyber Security practice. It will also provide you with the confidence to undertake further studies related to your academic practice and support you disseminating of this work.

Aims

This programme aims to prepare you with the knowledge, skills and values needed for a technical career with a specialism in cyber security by

- equipping you with a breadth of knowledge, skills and techniques needed as a professional in computer science
- developing your knowledge in specialised and advanced topics in cyber security
- enabling you to work with and learn from active researchers in computer science and cyber security
- enable you to critically evaluate the technical, social and management dimensions of computing systems and technologies from a security perspective

WHAT WILL I BE EXPECTED TO ACHIEVE?

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

Knowledge and understanding:

- demonstrate knowledge and understanding of and the ability to use advanced computing methods and techniques
- review and critically evaluate current challenges in cyber security, such as evaluating the security of a system or efficient approaches to digital forensics
- define and solve practical security problems based on underlying theoretical considerations
- select and apply leading-edge security techniques to practical tasks
- understand professional, legal, social, cultural and ethical issues related to computing and security and be aware of societal and environmental impact

Skills:

- analyse, select and develop solutions to security problems
- evaluate complex computer programs and systems in ways applicable to high security systems
- communicate topics in cyber security effectively to technical and non-technical audiences
- engage in critical peer review process of papers, software and proposals, and give positive advice for improvement and innovation

Values and attitudes:

- embrace technical challenges as an opportunity for personal development
- be prepared to engage in continued learning in your later career
- rationally exploit both traditional and novel technological approaches
- rigorously assess alternative approaches and novel designs and implementations

- acquiring a technical goal and encourage and lead others in order to achieve it
- a professional and ethical approach to security in the global environment

This programme has been developed in consultation with leaders in the security profession from both industry and government.

HOW WILL I LEARN?

The teaching and learning methods used are such that the levels of both specialisation of content and autonomy of learning increase as you progress through the programme. This progress will be guided by active researchers in cyber security, culminating in your individual project, an original piece of research, conducted largely independently with appropriate academic supervision.

The standard format is that taught modules are delivered through a series of 20 hours of lectures and 10 hours of tutorials/laboratory sessions. Lectures are normally used to:
(a) present and explain the theoretical concepts underpinning a particular subject;
(b) highlight the most significant aspects of a module's syllabus; and
(c) indicate additional topics and resources for private study.
Tutorials are used to help you develop skills in applying the concepts covered in the lectures of the relevant module, normally in practical problem solving contexts. Laboratory sessions serve a similar purpose as the tutorials but their strategy is to demonstrate application of concepts and techniques through the use of state-of-the-art software development tools and environments.

You will be expected to undertake independent study and do substantial coursework assignments for each module, amounting approximately to 120 hours per module. The coursework takes many forms, including programs, theoretical work, and essays, and is primarily formative, but also contributes to module assessment.

Coursework will be used in a coherent manner across all of the security specific modules to ensure that you will also get appropriate hands-on operational experience of relevant aspects of cyber-security, including testing and analysis. Some of this course work may be organised in ways that shadow larger scale exercises, such as the Cyber-Security Challenge. In particular in term 1, you will be divided into groups and you will become ethical hackers while attacking a particular computing infrastructure. In term 2, you will be asked to analyse and identify footprints of actual attacks.

The individual project is a substantial task that develops a research related topic and is performed under the supervision of academic staff, typically the researcher or a member of the research group that you have been associated with. The assessment of projects relies on a project report and a presentation. The individual project is supported by project preparation classes and individual supervision sessions. More information about the project/dissertation (INM363) criteria expected by the Department of Computer Science and the School can be found in our online tool MOODLE.

In addition to lecture, laboratory and tutorial support, the programme is supported by City's Moodle learning environment, which provides resources on each of the modules.

WHAT TYPES OF ASSESSMENT AND FEEDBACK CAN I EXPECT?

Assessment and Assessment Criteria

Assessment Criteria are descriptions, based on the intended learning outcomes, of the skills, knowledge or attitudes that you need to demonstrate in order to complete an assessment successfully, providing a mechanism by which the quality of an assessment can be measured. Grade-Related Criteria are descriptions of the level of skills, knowledge or attributes that you need to demonstrate in order achieve a certain grade or mark in an assessment, providing a mechanism by which the quality of an assessment can be measured and placed within the overall set of marks. Assessment Criteria and Grade-Related Criteria will be made available to you to support you in completing assessments. These may be provided in programme handbooks, module specifications, on the virtual learning environment or attached to a specific assessment task.

The assessment criteria will reflect the learning outcomes of the modules and the programme as a whole,

Feedback on assessment

Feedback will be provided in line with our Assessment and Feedback Policy. In particular, you will normally be provided with feedback within three weeks of the submission deadline or assessment date. This would normally include a provisional grade or mark. For end of module examinations or an equivalent significant task (e.g. an end of module project), feedback will normally be provided within four weeks. The timescale for feedback on final year projects or dissertations may be longer. The full policy can be found at University's website under the Assessment section.

Assessment Regulations

In order to pass your Programme, you should complete successfully or be exempted from the relevant modules and assessments and will therefore acquire the required number of credits.

The Pass mark for each module is 50%.

If you fail an assessment component or a module, the university regulations apply. In particular:

1. Compensation: where you fail up to a total of 20 credits at first or resit attempt (15 for a Postgraduate Certificate), you may be allowed compensation if:
   - Compensation is permitted for the module involved (see the module specification), and

- It can be demonstrated that you have satisfied all the Learning Outcomes of the modules in the Programme, and
- A minimum overall mark of no more than 10 percentage points below the module pass mark has been achieved in the module to be compensated, and
- An aggregate mark of 50% has been achieved overall.

If you receive a compensated pass in a module you shall be awarded the credit for that module. The original component marks shall be retained in the record of marks and the greater of the original module mark and the minimum pass mark for the module shall be used for the purpose of calculation towards the Award.

2. Resit: you will normally be offered one resit attempt. However, if you did not participate in the first assessment and have no extenuating circumstances, you may not be offered a resit.

If you are successful in the resit, you shall be awarded the credit for that module. The mark used for the purpose of calculation towards your Award shall be calculated from the original marks for the component(s) that you passed at first attempt and the minimum pass mark for the component(s) for which you took a resit.

If you do not satisfy your resit by the date specified you will not progress and the Assessment Board shall require that you withdraw from the Programme.

If you fail to meet the requirements for the Programme, but satisfy the requirements for a lower-level Award, then a lower qualification may be awarded as per the table below. If you fail to meet the requirements for the Programme and are not eligible for the award of a lower level qualification, the Assessment Board shall require that you withdraw from the Programme.

If you would like to know more about the way in which assessment works at City, please see the full version of the Assessment Regulations at:
http://www.city.ac.uk/__data/assets/word_doc/0003/69249/s19.doc

WHAT AWARD CAN I GET?

Master's Degree:

	HE Level	Credits	Weighting (%)
Taught	7	120	67
Dissertation	7	60	33

Class	% required
With Distinction	70
With Merit	60
With Pass	50

Postgraduate Diploma:

	HE Level	Credits	Weighting (%)
Taught	7	120	100

Class	% required
With Distinction	70
With Merit	60

With Pass	50

Postgraduate Certificate:

	HE Level	Credits	Weighting (%)
Taught	7	60	100

Class	% required
With Distinction	70
With Merit	60
With Pass	50

WHAT WILL I STUDY?

Taught component

There are in total 8 taught modules, 7 core modules and 1 elective module.

Module Title	SITS Code	Module Credits	Core/ Elective	Compensation Yes/No	Level
Information Security Fundamentals	INM440	15	Core	Yes	7
Network Security	INM441	15	Core	Yes	7
Security Auditing and Certification	INM442	15	Core	Yes	7
Research Methods and Professional Issues	INM373	15	Core	Yes	7
Cryptography	INM443	15	Core	Yes	7
Digital Forensics	INM445	15	Core	Yes	7
Cyber Crime and Sociotechnical Risk	INM446	15	Core	Yes	7
Object Oriented Programming in C++	INM359	15	Elective	Yes	7
Advanced Algorithms and Data Structures	INM422	15	Elective	Yes	7
Machine Learning	INM431	15	Elective	Yes	7
Principles of Data Science	INM430	15	Elective	Yes	7

**Elective choice may be constrained by timetabling requirements. The full range of electives may not be available in all years.*

Dissertation component

Module Title	SITS Code	Module Credits	Core/ Elective	Compensation Yes/No	Level
Individual Project	INM363	60	Core	No	7

You are normally required to complete all the taught modules successfully before progressing to the dissertation.

TO WHAT KIND OF CAREER MIGHT I GO ON TO?

When you graduate with the MSc in Cyber Security, you would be expected to progress directly into either advanced technical roles or research in the domain of cyber security. These roles can be in a broad range of areas, including all forms of software or hardware development and security applications in government and industry, such as computer security practitioner, security auditor, security architect, network security manager.

If you would like more information on the Careers support available at City, please go to: http://www.city.ac.uk/careers/for-students-and-recent-graduates.

WHAT STUDY ABROAD OPTIONS ARE AVAILABLE?

- None

WHAT PLACEMENT OPPORTUNITIES ARE AVAILABLE?

You can participate in our professional placement programme, which is supported by the Professional Liaison Unit. This will enable you to undertake your final project within an industrial or research placement over an extended period compared to regular project.

WILL I GET ANY PROFESSIONAL RECOGNITION?

British Computer Society
- The programme is BCS accredited.
- Plan to submit programme for NCSC accreditation, course being designed to comply with draft standards

HOW DO I ENTER THE PROGRAMME?

Information on:
Entry requirements

Applicants should normally have a UK first or an upper second class honours degree (or equivalent) in computer science or a related discipline with some mathematical content.

Relevant industrial experience may also be considered for entry to this course.

For those overseas applicants, whose first language is not English or their country has not been exempted from the English language requirement by the UK Home Office, they will need to provide one of the following English test qualifications:

- IELTS: 6.5 (minimum of 6.0 in all four components)
- TOEFL 92 (minimum of 20 in Listening, Reading and Speaking, and 22 in Writing)

Scholarships (including any institution-wide scholarships)

- Standard for SMCSE MSc

Version: 7.0
Version date: May 2020
For use from: 2020-21