MSc Cyber Security and Pen Testing

Programme Specification

1. Programme title	MSc Cyber Security and Pen Testing
2. Awarding institution	Middlesex University
3. Teaching institution	*Middlesex University: London* *Middlesex University: Malta* *Middlesex University: Dubai* *Middlesex University: Mauritius*
4. Details of accreditation by professional/statutory/regulatory body	
5. Final qualification	MSc Cyber Security and Pen Testing, PGDip Cyber Security and Pen Testing & PGCert Cyber Security and Pen Testing
6. Year of validation	2018/19
Year of amendment	2019/20
7. Language of study	English
8. Mode of study	Full-Time & Part-Time

9. Criteria for admission to the programme

A minimum of a second-class Honours degree (UK), or an equivalent overseas qualification – in computer science or in a science or engineering related subjects. Candidates with other degrees but with relevant work experience may also be considered and are encouraged to apply.

Whilst consideration of Recognition of Prior Learning (RPL) has been given, the programme team decided that it will not be accepted for candidates admitted onto this programme.

International students whose first language is not English or who have not been taught in the English medium throughout, and whose first degree is not from a British

university, must achieve an IELTS score of 6.5 with a minimum score of 6 in each band.

10. Aims of the programme

The programme aims to equip students with:

- An understanding of the fundamental importance of computer, network, and communication system security for an organisation.
- The ability to involve both the management and the user in the process of awareness, decision and implementation with regard to computer and network security.
- The skills to analyse the security risks a communication system may have and to propose/devise solutions.
- The knowledge necessary to evaluate new threats to authentication, confidentiality and privacy with a view of implementing solutions to combat such threats.
- The ability to make a functional security design for a communication system and implement it successfully.
- A balance of theory, advanced practical skills and experience to enable students to develop a sound knowledge and analytical ability to facilitate their intellectual and professional development.

11. Programme outcomes*

A. Knowledge and understanding	**Teaching/learning methods**
On completion of this programme the successful student will have knowledge and understanding of : 1. Algorithms used in computer and network security and be able to perform implementations of selected algorithms in this area together with their potential for increased organisational efficiency. 2. Threats faced by computer operating systems, applications and networks and various countermeasures that can be used 3. Analysis, design and implementation of security systems, with an	Students gain knowledge and understanding through Self-directed study, resource based learning, small group discussions, small group and individual exercises, online laboratory sessions, live demonstration software, on-line examples and research project. Weekly seminar sessions that provide students with the opportunity to address questions, queries and problems. • Traditional lecture delivery (outcomes 1-10), • Group and individual research, presentations and written reports (outcomes 1-9), • Laboratory sessions (outcome 2, 5 & 6).

understanding of how cryptography can be used for providing security within applications. 4. Analysing a problem specification and to design and implement a solution. 5. Relevant professional, ethical and legal issues in computer and network security 6. A range of problems of computer and network security, and the available solutions and trade-offs 7. Applying secure methods for transmission and storage of data 8. To become familiar with different research methods to develop policies and select suitable mechanisms to enforce such policies 9. Full knowledge and understating of rules and regulations pertaining to cyber security 10. Ability to apply technical strategies, tools and techniques to secure data and information for customers/clients	• Individual and group design work (outcomes 3, 4, 5, 8 -10), • Individual project. Throughout the students are encouraged to undertake independent reading both to supplement and consolidate what is being taught/learned and to broaden their individual knowledge and understanding of the subject (outcomes 1-10). **Assessment methods** Students' knowledge and understanding is assessed by: Group and individual coursework, presentations, group and individual reports, and the unseen examination and the project thesis assess students' knowledge and understanding. • Outcomes 1-7 assessed by examination. • Outcomes 3 and 6 are assessed by laboratory sessions and practical assignments • Outcome 1-10 are assessed by individual essay and final project thesis.
B. Skills On completion of this programme the successful student will be able to: 1. Critically evaluate the needs for security provision for communication networks and apply security policies and regulations for existing security systems. 2. Have a critical and clear understanding of current theories and techniques for apprising user interfaces and practical designs skills for effective user interactions 3. Critically analyse and evaluate security applications and techniques and	**Teaching/learning methods** Students learn cognitive skills through • traditional lecture delivery (outcomes 1 and 3), • Group and individual research, presentations and written reports (outcomes 1-5), • Small group and individual exercises (outcomes 1-6), • Live virtual online Laboratory sessions (outcome 4 and 5), • Individual project (outcomes 1-6 and 8-13: depending on project title).

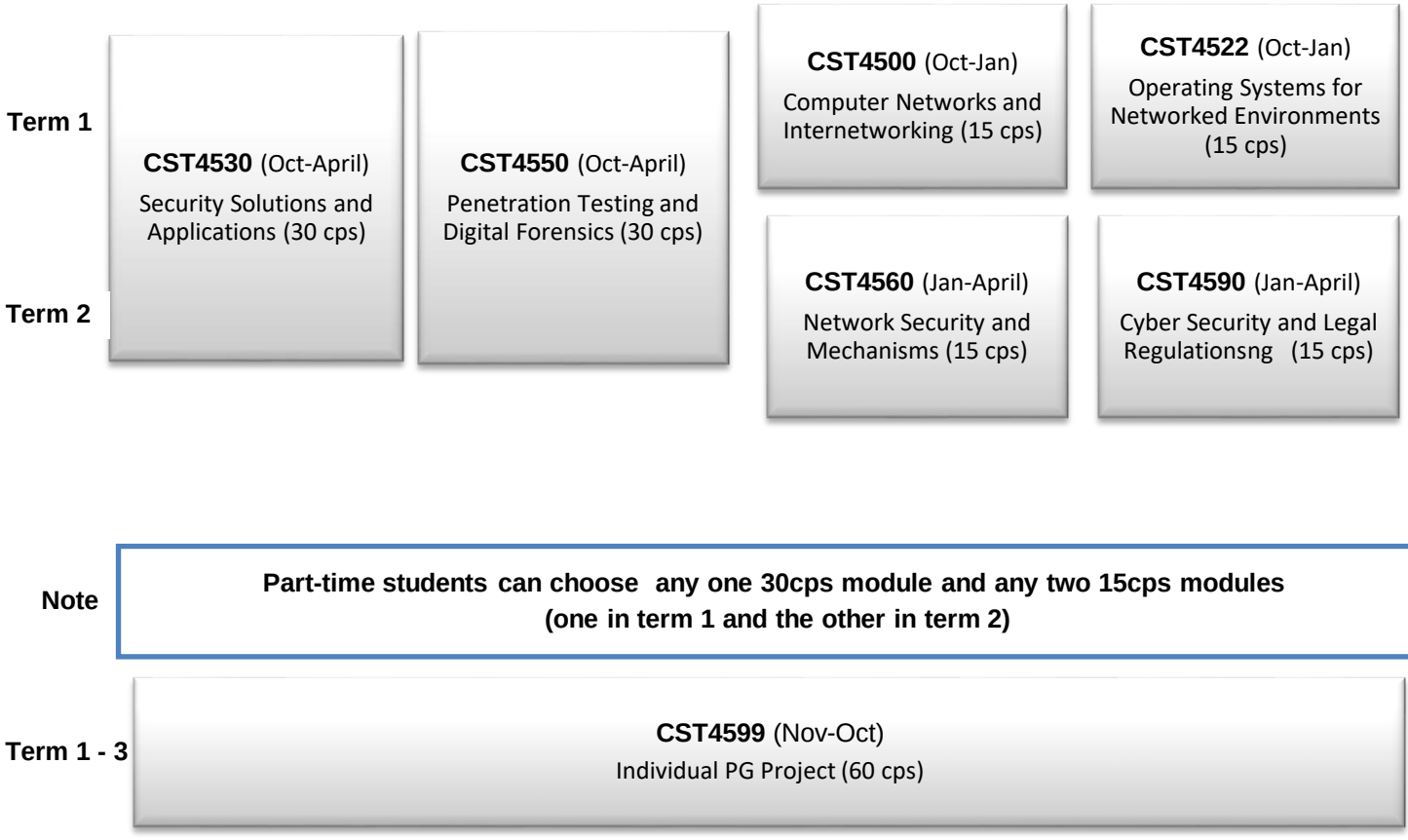
recommend and propose new measures to improve security 4. Make informed choices of the appropriate security measures to put into place for a given network and/or an operating system 5. Demonstrate fundamental security management skills and techniques relating to the leadership of projects. 6. Draw up security measures for computer networks and communication systems 7. Acquire and apply relevant mathematical techniques to carry out security algorithms 8. Analyse a problem systematically and implement an effective solution both individually and within a group 9. Communicate effectively with peers and senior managers in writing, verbally and through graphical notations. 10. Apply learnt knowledge in computer and network security to better protect a networking environment	Analysis, design and problem solving skills are further developed through various design activities as well as case studies, and extensive computer laboratory sessions. Feedback is given to students on all assessed coursework as well as written exams (In the form of exam reports produced each term). **Assessment methods** Students' cognitive skills are assessed by: • Group and individual coursework (outcomes 1-6) • Laboratory tests (outcome 1, 4-5), • The unseen examination (outcomes 1-6 and 7), and • The project thesis (outcomes 1-6 and 8-10 depending on project title) • Skills 7-10 are assessed through coursework and written exam (seminars) • Skills 8-10 are assessed by laboratory sessions.

12. Programme structure (levels, modules, credit points (CPS) and progression requirements)

12. 1 Overall structure of the programme

Your Modules

Full-Time/ Part-Time



12.2 Levels and modules
Starting in academic year 2010/11 the University is changing the way it references modules to state the level of study in which these are delivered. This is to comply with the national Framework for Higher Education Qualifications. This implementation will be a gradual process whilst records are updated. Therefore the old coding is bracketed below.

Level 7

COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS
Students must take all of the following: Students must take all of the following: **CST4500:** Computer Networks and Internetworking **CST4522:** Operating Systems for Networked Environments **CST4530:** Security Solutions and Applications **CST4550:** Penetration Testing and Digital Forensic**s** **CST4560:** Network Security and Mechanisms **CST4590:** Cyber Security and Legal Regulations **CST4599:** Individual PG Project	There are no optional modules on this programme	**Students must <u>pass all the taught modules and submit a formal proposal</u> before they can progress onto the project.** **To pass a module, students must pass all components of assessment (i.e. examinations, coursework)**

12.3 Non-compensatable modules (note statement in 12.2 regarding FHEQ levels)

Module level	**Module code**
7	CST4550: Penetration Testing and Digital Forensics
7	CST4599: Individual PG Project

13. Curriculum map

See attached.

14. Information about assessment regulations

Compulsory modules are those that must be taken; that is, the qualification cannot be made unless these modules have been successfully completed.

Each of these modules makes a unique contribution to the learning objectives of the programme.

- Information on how the University formal assessment regulations work, including details of how award classifications are determined, can be found in the University Regulations at www.mdx.ac.uk/regulations/.
- Modules are assessed in accordance with the Faculty of Science and Technology assessment strategy. Most modules adhere to a standard pattern of final grades being made up of examinations and/or coursework.
- Practical aspects of the programme are often assessed via coursework that may be carried out using specialist software and may include lab tests.
- Theoretical material is normally assessed by a combination of both coursework and examination at level 7.
- Grades are awarded on the standard University scale of 1–20, with Grade 1 (80-100%) being the highest. To pass a module all components, both coursework and examination, must be passed individually with a minimum grade of 16 (40%). Failure in one of the components will result in the failure of the module.
- For additional information on assessment and how learning outcomes are assessed please refer to the individual module narratives for this programme.

15. Placement opportunities, requirements and support

Not applicable

16. Future careers (if applicable)

All programmes in the Faculty of Science & Technology – their curricula and learning outcomes – have been designed with an emphasis on currency and the relevance to future employment.

- Campus Career Offices can be found on campus for advice, support and guidance.
- The majority of graduates are employed in IT posts relevant to the subject.
- Over 20% of students pursue further postgraduate study or research.
- The Faculty has an Industrial Advisory Group which meets to advise and inform the department and the faculty.

The employer links with the faculty are encouraged and take part in a number of ways:

- by inviting practitioners from industry as guest speakers in lectures;
- through links with companies where students are employed as alumni both in the UK and overseas.

17. Particular support for learning (if applicable)

In support of the student learning experience:
please check this link: http://unihub.mdx.ac.uk/study

- The Faculty's teaching and Learning Strategy is compliant with those of the University, in seeking to develop learner autonomy and resource-based learning. In support of the students learning experience:

- All new students go through an induction programme and some have early diagnostic numeric and literacy testing before starting their programme. The Learner Development Unit (LDU) provides one-to- one tutorials and workshops for those students needing additional support in these areas.
- Students are allocated a personal email account, secure networked computer storage and dial-up facilities
- A programme handbook is made available to students at enrolment (electronic copies for all students are available via virtual learning environment).
- New and existing students are given module handbooks for each module they study. Soft copies of all module handbooks can be found on Unihub. Web-based learning materials are provided to further support learning.
- Extensive library facilities are available at the base campus.
- Students can access advice and support on a wide range of issues from the Student Services Counter and the Student Information Desk. Student Advisers aligned to subject areas offer confidential one to one advice and guidance on programme planning (if applicable) and regulations.
- High quality specialist laboratories equipped with industry standard software and hardware where appropriate, for formal teaching as well as self-study.
- Tutorial sessions for each module organised for groups of up to 20 students are provided for additional teaching support.
- Formative feedback is given on completion of student coursework
- Past exam papers for all modules (which are assessed by examination) are available for students via Unihub.
- Research activities of academic staff feed into the teaching programme, which can, on some occasions, provide an opportunity for students to work with academics on some aspect of research.

Middlesex University encourages and supports students with disabilities. Some practical aspects of Faculty of Science & Technology programmes may present challenges to students with particular disabilities. You are encouraged to contact us at any time to talk in confidence about your needs. If we know your individual needs we'll be able to provide for them more easily. For further information contact the Disability Support Service (email: disability@mdx.ac.uk).

Access to some on-campus facilities may be restricted due to Covid-19.

18. JACS code (or other relevant coding system)	011I108, 011I109, 011I110
19. Relevant QAA subject benchmark group(s)	Computing

20. Reference points

The following reference points were used in designing and reviewing the programme:

- QAA Framework for Higher Education Qualification in England, Wales and Northern Ireland
- QAA Computing subject benchmarks
- QAA/QAAS guidelines for programme specification
- QAA Code of Practice for the assurance of academic quality and standards in HE
- University' Policy, Regulations and guidelines
- British Computer Society (BCS) Guidelines for Exemption and Accreditation
- Middlesex University and School of Science & Technology
- Teaching Learning and Assessment policies and strategies
- University policy on equal opportunities.

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if s/he takes full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

Curriculum map for *MSc Cyber Security and Pen Testing Programme*

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.

Programme learning outcomes

Knowledge and understanding	
A1	Algorithms used in computer and network security and be able to perform implementations of selected algorithms in this area together with their potential for increased organisational efficiency.
A2	Threats faced by computer operating systems, applications and networks and various countermeasures that can be used
A3	Analysis, design and implementation of security systems, with an understanding of how cryptography can be used for providing security within applications.
A4	Analysing a problem specification and to design and implement a solution.
A5	Relevant professional, ethical and legal issues in computer and network security
A6	A range of problems of computer and network security, and the available solutions and trade-offs
A7	Applying secure methods for transmission and storage of data
A8	To become familiar with different research methods to develop policies and select suitable mechanisms to enforce such policies
A9	Full knowledge and understating of rules and regulations pertaining to cyber security
A10	Ability to apply technical strategies, tools and techniques to secure data and information for customers/clients
Skills	
B1	Critically evaluate the needs for security provision for communication networks and apply security policies and regulations for existing security systems.

B2	Have a critical and clear understanding of current theories and techniques for apprising user interfaces and practical designs skills for effective user interactions
B3	Critically analyse and evaluate security applications and techniques and recommend and propose new measures to improve security
B4	Make informed choices of the appropriate security measures to put into place for a given network and/or an operating system
B5	Demonstrate fundamental security management skills and techniques relating to the leadership of projects.
B6	Daw up security measures for computer networks and communication systems
B7	Acquire and apply relevant mathematical techniques to carry our security algorithms
B8	Analyse a problem systematically and implement an effective solution both individually and within a group
B9	Communicate effectively with peers and senior managers in writing, verbally and through graphical notations.
B10	Apply learnt knowledge in computer and network security to better protect a networking environment

Programme outcomes																		
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10

Highest level achieved by all graduates																			
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Module Title	Module Code by Level	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Computer Networks and Internetworking	CST4500	✓	✓	✓		✓	✓	✓		✓			✓			✓	✓	✓	✓	✓	
Operating Systems for Networked Environments	CST4522		✓		✓	✓	✓	✓	✓		✓						✓	✓	✓	✓	
Security Solutions and Applications	CST4530	✓		✓		✓				✓	✓	✓		✓	✓	✓		✓			✓
Penetration Testing and Digital Forensics	CST4550	✓		✓	✓		✓		✓				✓				✓	✓			
Network Security and Mechanisms	CST4560		✓			✓		✓		✓				✓			✓	✓		✓	✓
Cyber Security and Legal Regulations	CST4590				✓	✓						✓	✓	✓	✓		✓		✓		
Individual PG Project	CST4990	✓	✓			✓		✓	✓	✓	✓				✓	✓			✓	✓	✓