PROGRAMME DETAILS
Programme Code: F2N3-CNS
Department: Computer Science
Main Award: MSC - Master of Science
Full Award Title: Master of Science in Network Security
Level: Postgraduate Taught

LOCATION OF STUDY
<table>
<thead>
<tr>
<th>Location</th>
<th>Edinburgh</th>
<th>Scottish Borders</th>
<th>Orkney</th>
<th>Dubai</th>
<th>Malaysia</th>
<th>Approved Learning Partner</th>
<th>Independent Distance Learners</th>
<th>Other</th>
</tr>
</thead>
</table>

ASSOCIATED AWARDS

<table>
<thead>
<tr>
<th>Programme Code</th>
<th>Award</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>F2A3-ZZZ</td>
<td>PGCERT</td>
<td>Postgraduate Certificate in Computer Science</td>
</tr>
<tr>
<td>F2N2-CNS</td>
<td>PGDIP</td>
<td>Postgraduate Diploma in Network Security</td>
</tr>
<tr>
<td>F2N3-CNS</td>
<td>MSC</td>
<td>Master of Science in Network Security</td>
</tr>
</tbody>
</table>

ACCREDITATION
N/A

LEARNING OUTCOMES – SUBJECT MASTERY

Understanding, Knowledge and Cognitive Skills

- Critical understanding of the main theories, principles and concepts relating to the domain of computer network security including conventions, methodologies, standards and terminology.
- Understanding and use of a significant range of the main practices, skills and techniques in network security software engineering, and a range of specialised skills, research and investigation techniques, and practices in designing and validating computer network security solutions informed by current best practice.
- Broad and deep knowledge of the computer network security areas of access control, cryptography, means of authentication, network security tools, security policy management, as well as application-based knowledge and skills relating to known security exploits, malware and their detection and prevention, and specialist knowledge and skills in applications relating to a number of specialist areas such as biometrics, firewall management, intrusion detection, penetration testing, public key certificates and user education in good security practice.

Scholarship, Enquiry and Research (Research Informed Learning)

- Extensive, detailed and critical understanding of at least one specialist area within the domain of Computer Network Security application development obtained through researching the background to a substantial and challenging network security engineering project that addresses a real or simulated sets of threats by personal scholarship, design, development and testing of a detailed means of prevention.
- Detailed knowledge and understanding of network security software engineering techniques relating to authentication, authorisation and auditing as well as the practical skills in how to exploit them in support of original and creative network security application development.
- Specialist and critical knowledge, understanding and skills in a number of mainstream and specialist areas within the domain of network security application development including cryptography, digital forensic techniques, malware analysis, network defence technologies and penetration testing.

LEARNING OUTCOMES – PERSONAL ABILITIES

Industrial, Commercial and Professional Practice
Demonstrate critical awareness of current issues within network security application development, and make informed judgements about them in the light of relevant professional standards.

- Demonstrate an awareness of professional and research issues in the network security discipline, and an ability to critique current techniques and practice.

**Autonomy, Accountability and Working With Others**

- Work autonomously and within teams, as appropriate, demonstrating a capability for both taking and critically reflecting on roles and responsibilities.
- Develop and utilise advanced problem-solving skills and techniques in the shared development of original and creative solutions to general and specialist network security engineering issues.
- Develop and demonstrate skills and techniques in communication with peers and academic/industrial staff, using a range of appropriate methods to suit different levels of knowledge and expertise within the audience.

**Communication, Numeracy & Information and Communications Technology**

- Develop and demonstrate the ability to communicate and present the main issues involved in network security application development to a literate audience with appropriate use of modern presentational tools and aids.
- Demonstrate appropriate use of methods of calculation and estimation involved in planning network security engineering solutions and deploying and validating such solutions.

**APPROACHES TO TEACHING AND LEARNING**

This programme is offered in a traditional campus-based, cohort model. Within the timetable, courses offer traditional lecture-based materials, small group tutorials and a variety of laboratory-based practicals. Students are expected to complete coursework in groups, teams and pairs, as well as individually, and courses offer a range of types of coursework for assessment, from discursive essay-style assignments to code design and generation. In some courses, team teaching approaches are adopted to provide additional support and variety, and electronic support, in the form of email lists, newsgroups and bulletin boards are widely used to disseminate information and support student communication and practice.

**EDUCATIONAL AIMS OF THE PROGRAMME**

- Detailed knowledge and critical understanding of the main areas of computer network security including theories, principles and concepts.
- Significant range of principal and specialist skills, techniques and practices in the computer network security domain.
- Specialist knowledge of security techniques as they apply to developing distributed and networked applications.
- Ability to critically review existing practice and develop original and creative solutions to problems requiring computer network security solutions.
- Ability to communicate and work effectively with peers and academic staff in a variety of tasks, demonstrating appropriate levels of autonomy and responsibility.
- Ability to plan and execute a significant project of research, investigation or development in a specialist area within computer network security, demonstrating extensive, detailed and critical understanding of that specialism.

**ASSESSMENT POLICIES**

Postgraduate programmes consist of two phases:
• A *taught phase*, consisting of a set of 8 taught courses, some mandatory and some optional, defined in the programme structure, which the students will study over two semesters. Assessment of the taught phase is through a variety of methods including coursework and/or examination. Students must submit all elements of assessment before being permitted to progress.

• A *dissertation phase*, consisting of an appropriate technical research project and project dissertation report.

• Students will normally complete the taught phase, at which point progression to the dissertation phase is dependent on assessed performance as being of Masters level standard. To progress students must get grade D or better in the 8 taught courses, get a taught course average of 50% and pass F21RP with a mark of at least 45%.

• Any student will be able to retake the assessment of up to a maximum of 3 courses at the next opportunity, subject to payment of the appropriate fees to the University, and may be required to do so to obtain the necessary credits for completion of their programme or for progression. Students may only resit courses for which their examination grade is E or F (or a D but only if that is required for them to qualify for an MSc degree). The method of reassessment for each course is specified in the appropriate course descriptor.

• Students meeting the required standards for Postgraduate Diploma and Postgraduate Certificate in the taught phase, but not meeting the Masters standard, will not be permitted to progress to the dissertation phase. Students may be recommended to graduate with a Postgraduate Diploma or a Postgraduate Certificate at this point.

• Students failing to meet the required standards for Postgraduate Diploma and Postgraduate Certificate in coursework and examination in the taught phase will not be permitted to progress to the dissertation phase, nor will they be eligible for any award.

### PROGRAMME STRUCTURE

#### Mandatory Courses

<table>
<thead>
<tr>
<th>Edinburgh</th>
<th>SBC</th>
<th>Orkney</th>
<th>Dubai</th>
<th>HWUM</th>
<th>IDL</th>
<th>Coll. Partner</th>
<th>ALP</th>
<th>Other</th>
<th>Stage</th>
<th>Semester</th>
<th>Course Code</th>
<th>Course Title</th>
<th>SCQF Cr</th>
<th>SCQF Lvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21CN</td>
<td><strong>Computer Network Security</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>F21AN</td>
<td><strong>Advanced Network Security</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>F21RP</td>
<td><strong>Research Methods and Project Planning</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>3</td>
<td>F21MP</td>
<td><strong>Masters Project and Dissertation</strong></td>
<td>60</td>
<td>11</td>
</tr>
</tbody>
</table>

#### Optional Courses

<table>
<thead>
<tr>
<th>Edinburgh</th>
<th>SBC</th>
<th>Orkney</th>
<th>Dubai</th>
<th>HWUM</th>
<th>IDL</th>
<th>Coll. Partner</th>
<th>ALP</th>
<th>Other</th>
<th>Stage</th>
<th>Semester</th>
<th>Course Code</th>
<th>Course Title</th>
<th>SCQF Cr</th>
<th>SCQF Lvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>B31TF</td>
<td><strong>Sensors, Actuators and IoT</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21DF</td>
<td><strong>Databases and Information Systems</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21DL</td>
<td><strong>Data Mining and Machine Learning</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21RS</td>
<td><strong>Rigorous Methods for Software Engineering</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21SC</td>
<td><strong>Industrial Programming</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F21SF</td>
<td><strong>Software Engineering Foundations</strong></td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>F29DC</td>
<td><strong>Data Communications and Networking</strong></td>
<td>15</td>
<td>9</td>
</tr>
</tbody>
</table>
8 taught courses (4 mandatory + 4 optional) plus a dissertation.

Delivery of F21SF Software Engineering Foundations and F21RS Rigorous Methods for Software Engineering in Edinburgh from 2018/19 onwards will now make them mutually exclusive courses in semester 1. This is done to allow them to be timetabled at the same time. It is not envisaged that there will be any demand by students to take both as they are aimed at students with very different programming capabilities. Programme descriptions made available to prospective and enrolled students to the Edinburgh campus are and will warn them that the 2 courses are mutually exclusive options. Dubai delivery of these courses will not be subject to this constraint.
1. A student who has been awarded a Grade E or F in a course may be re-assessed in that course. A student who has been awarded a Grade D in a course may be re-assessed in that course in order to proceed to or be eligible to receive the award of Masters.
2. A student shall be permitted only one re-assessment opportunity in a maximum of three taught courses. The opportunity for re-assessment in four or more taught courses shall be at the discretion of the Progression Board.
3. Any further re-assessment opportunities in a course will require the approval of the Postgraduate Studies Committee.
4. A student may be permitted, at the discretion of the Progression Board, to be re-assessed in the dissertation, project or other supervised research component of the course of study.

PROGRESSION TO DISSERTATION/PROJECT

Students may progress to the Dissertation if they have met the progression requirements (taught course credit weighted average of 50% or better, all courses at Grade D or above and 45% or better in F21RP)