
School of Engineering & Built Environment

# BEng (Hons) in
# Digital Security, Forensics & Ethical Hacking

## Programme Specification Proforma (PSP)

## August 2015

GLASGOW CALEDONIAN UNIVERSITY

# Programme Specification Pro-forma (PSP)

## 1. GENERAL INFORMATION

| | |
|---|---|
| **1. Programme Title:** | **BEng (Hons)**<br>Digital Security, Forensics and Ethical Hacking |
| **2. Final Award:** | **BEng (Hons)**<br>Digital Security, Forensics and Ethical Hacking<br>Digital Security, Forensics and Ethical Hacking (Sandwich)<br>Digital Security, Forensics and Ethical Hacking (Part-time) |
| **3. Exit Awards:** | CertHE & DipHE Network and Digital Security Technologies<br>BEng Digital Security, Forensics and Ethical Hacking<br>BEng Digital Security, Forensics and Ethical Hacking (Sandwich)<br>BEng Digital Security, Forensics and Ethical Hacking (Part-time) |
| **4. Awarding Body**: | Glasgow Caledonian University |
| **5. Approval Date:** | May 2011 |
| **6. Faculty/School:** | School of Engineering & Built Environment |
| **7. Host Department:** | Computer, Communications and Interactive Systems (CCIS) |
| **8. UCAS Code:** | I112 |
| **9. PSB Involvement:** | The Institution of Engineering and Technology (IET); The Chartered Institute for IT (BCS) |
| **10. Place of Delivery:** | GCU |
| **11. Subject Benchmark Statements**: | $EC^{UK}$ UK-SPEC |
| **12. Dates of PS Preparation/Revision**: | May 2011 |

## 2. EDUCATIONAL AIMS OF THE PROGRAMME

### 2.1 Programme Philosophy

The philosophy of the BEng/BEng (Honours) Digital Security, Forensics and Ethical Hacking programme is to provide a stimulating broad-based education through an integrated study of vocational and academic disciplines, providing students with an enjoyable and rewarding experience that places emphasis on active and participative learning. It is based on an industrial and business-related curriculum in the theory and practice of computer science and engineering with special emphasis in the area of digital forensics, security and ethical hacking.

The multidisciplinary programme aims to provide graduates with cognitive and practical skills and knowledge of new and emerging theories, methods and principles together with the practical ability to apply appropriate tools and techniques systematically. The aim is to establish graduates with the ability to resolve digital forensics and security problems, design, develop and manage computing and network solutions for the resolution of digital forensics and security activities, be knowledgeable of current and emergent technologies, understand legal, social, ethical and professional responsibilities of practitioners and have a broad awareness of industry. The programme will encourage students' creative thinking, develop visualization skills, expand knowledge, confidence and professional values so producing highly skilled and professional graduates able to pursue careers in cyber crime investigations and digital security.

The programme is taught within a wider programme of study related to the discipline of Secure Networked Systems Engineering. Sharing a common first two years within the suite, the programme provides an opportunity to explore specialisms within the general theme of Secure Networked Systems Engineering together with those that are core to the understanding of scientific and engineering disciplines, and technological principles. This provides students with experience of, and the opportunity to transfer to, other programmes within the suite.

The programme forms part of the School and the University's commitment to provide programmes that meet the demands for current and developing technologies in society, business and industry. The aim is to integrate the expertise of staff gained from research, consultancy and scholarly activity into the programme delivery as appropriate. The school has a strong ethos of providing career oriented learning experiences and has established itself as an approved provider for professional certifications, notably from Cisco, Microsoft, Oracle, and the leading Information Security and Computer Forensics firm, 7Safe. We aim to sustain existing, and seek further industrial partnerships that provide access to case studies and projects, work experience and real world problems. The new programme has been developed to address contemporary issues in the developing field of digital forensics and security. The School will work closely with Caledonian Business School in providing an inter-disciplinary approach, to teach risk management and the legal framework surrounding the use of computers, particularly with regard to privacy, freedom of information and powers of investigation.

Application of the programme philosophy will produce professionals who are able to combine established scientific and engineering professional good practice and technical skills with the ability to work effectively in the field of digital forensics, solving digital forensics problems, providing systems to address digital forensics issues, address issues associated with computer crime and enhance the quality of society by making computer systems more secure and robust. The programme equips graduates with the transferable skills required for future academic and personal development. The programme addresses the rapidly emerging need for skilled professionals in the developing specialist areas of digital forensics, digital security and ethical hacking. We would expect graduates to embark on a range of career pathways including

government agencies, law enforcement or associated private sector agencies, supporting specialist roles such as forensic practitioners, penetration testers (ethical hackers) and security and forensic consultants. The multidisciplinary nature of the programme provides a range of subjects to facilitate the development of abilities, pursuit of interests and promotion of wider career opportunities and choices.

The programme adopts the philosophy of providing an educational programme that incorporates the professional requirements throughout the module syllabus. The BEng exit pathways correspond with the graduate as technical specialist (supporting the need for technology "innovators") with technical expertise enhanced in selected niche areas. The programme has been designed to satisfy the requirements for professional membership of IET (Institute of Engineering and Technology) and BCS (The Chartered Institute for IT) accreditation to contribute to the expectations to provide partial fulfilment of the competence and commitment required to prepare graduates to progress to Chartered Engineer (CEng), Chartered IT Professional (CITP) and Chartered Scientist (CSci) status after gaining the necessary professional experience. There is an expectation students will exercise leadership, initiative, personal responsibility and decision making in complex and unpredictable situations.

## 2.2 General Aims of the Programme

The programme aims to provide graduates with cognitive, practical, self-management skills and knowledge of theoretical, professional, technical, legal and social aspects to be able to pursue careers in computer crime investigations and digital security. It aims to provide graduates with:

- A stimulating curriculum which combines study of core technological concepts, theories and principles in addition to specialised knowledge and understanding in the area of digital forensics, digital security and ethical hacking enabling graduates to make a significant contribution to industry and society as professional practitioners;
- An understanding of scientific and engineering systems approaches encompassing the themes of digital forensics, security technologies, programming for networks, security systems theory, communications networks and the practicalities of information and security systems, including compliance with appropriate standards in order to cope adequately with current and emerging technologies;
- A range of analytical and modelling methods for use in scientific and engineering applications within the forensics and security specialisms to specify and design secure digital networks and systems;
- Skills to identify, analyse, specify, design, test and implement information systems and security of an organisation to support achievement of its business goals, and to specify and develop elements of a secure digital system, integrating hardware, software and business elements;
- A range of problem solving strategies to enable the application of knowledge in a flexible manner;
- The ability to think clearly, rationally, logically, and draw independent conclusions based on rigorous, analytical and critical assessment of arguments, opinions and data;
- Skills in the use of digital technologies and relevant aspects of information technology;
- An understanding of the legal and ethical issues and concepts relating to digital systems and security, together with the audit procedures for assessing security systems and controls;
- An awareness of the social impact of digital forensics and digital security, together with the ability to act in a professional and ethical manner in the development and use of digital

systems, in general, and in the analysis, documentation and presentation of digital forensics cases in particular;

- The skills that enables effective communication (in writing and orally) at the appropriate business and technical level with users, management, customers and technical specialists in such a way as to meet legal regulations, requirements and audit trails and be able to present digital evidence in court;
- An extension of analytical, creative and intellectual skills to enhance and improve judgement in decision making;
- The opportunities to develop interpersonal and key soft skills, through significant exposure to team based projects and problem based learning;
- A sound understanding and awareness of commercial, social and business factors which influence technical solutions to solve problems, through exposure to the CISCO Entrepreneurship Institute;
- A range of general transferable and marketable skills, knowledge relevant to employment in a variety of roles both within the field and associated industries, together with the personal attitudes and determination necessary for professional development and further study to enable the student to make a valuable contribution throughout a successful career.

## 3. PROGRAMME STRUCTURES AND REQUIREMENTS, LEVELS, MODULES, CREDITS AND AWARDS

3.1 Full-Time and Sandwich Programme Curriculum

| YEAR | RELATED MODULES | TRIMESTER | CREDITS |
|---|---|---|---|
| YEAR 1 | M1I322909 Programming 1 | A | 20 |
| | M1I123711 Introduction to Computer Networking | A | 20 |
| | M1I322910 Web Platform Development 1 | B | 20 |
| | M1I322997 Integrated Project 1 | B | 20 |
| | M1I322951 Mathematics for Computing | AB | 20 |
| | M1I323146 Fundamentals of Computing | AB | 20 |
| | | | |
| | | | |
| YEAR 2 | M2G421117 Operating Systems & Security | A | 20 |
| | M2G405208 Routing Fundamentals | A | 20 |
| | M2G421123 Digital Forensics Essentials & Incident Response | A | 20 |
| | M2H620655 Integrated Design Project 2 | B | 20 |
| | M2I322954 Database Development | B | 20 |
| | M2G421127 Designing Secure Networks | B | 20 |
| | | | |
| | | | |
| YEAR 3 | M3G121115 Quantitative Modelling and Cryptography | A | 20 |
| | M3I123695 Digital Forensics Analysis | A | 20 |
| | M3I123698 Network Penetration Testing and Ethical Hacking | A | 20 |
| | M3M121130 Regulating the Information Society | B | 20 |
| | M3H620657 Integrated Design Project 3 | B | 20 |
| | M3I123696 Advanced Ethical Hacking & Web Application Penetration Testing | B | 20 |
| | | | |
| | | | |
| YEAR 4 | MHG405297 Honours Research and Project Methods | A | 10 |
| | MHI223288 Malware Analysis and Reverse Engineering | A | 20 |
| | MHG122335 Cloud Systems Security | A | 20 |
| | MHI123697 Mobile Device Security, Forensics & Penetration Testing | B | 20 |
| | MHH620649 Professionalism in Practice | AB | 10 |
| | M HG405293 Honours Project | AB | 40 |

| | ***Notes:*** |
|---|---|
| **1.** | ***Student Exchange (Optional).*** After successful completion of Level 3 Trimester 1 students maybe eligible to undertake an optional study exchange during Trimester 2 at an appropriate host Institution outwith the UK, provided the agreed programme of activity is equivalent to the curriculum and intended student experience normally undertaken in Level 3 Trimester 2. Successful completion of the study exchange is credit bearing to 60 credits. |
| **2.** | ***Industrial Placement Year (Optional) Exit Award.*** Students opting to undertake placement do so in the academic session after Level 3 studies. Assessment is via the additional 60 SCOTCAT level 3 credit module, M3H105245 Applied Computer Based Systems Engineering Practice. Successful completion of that module gives (Sandwich) in the final exit award obtained by the student. |

ASSESSMENT REGULATIONS

The Glasgow Caledonian University Assessment Regulations apply to this programme.