THE UNIVERSITY of EDINBURGH
College of Science & Engineering

Proposal for New Degree Programmes

Stage 2

Contents

THE UNIVERSITY OF EDINBURGH

PROGRAMME SPECIFICATION FOR [*INSERT NAME OF PROGRAMME OF STUDY, e.g.* M.A. Honours in Ancient History *or* M.Sc. in Public Health][1]

PROGRAMME SPECIFICATION

Grey text has been added to provide guidance. Please delete as you add your own text, remove italics, and change the font colour to black.

OVERVIEW	
Awarding Institution	University of Edinburgh
Teaching Institution	University of Edinburgh
Programme accredited by	n/a
Final Award	PhD
Programme Title	PhD in Security, Privacy and Trust
UCAS Code	n/a
Relevant QAA Subject Benchmarking Group(s)	**n/a**
Postholder with overall responsibility for QA	Director of Training
Date of Production/revision	3/12/2018

[1] The information contained in this Programme Specification should be used as a guide to the content of a degree programme and should not be interpreted as a contract.

EXTERNAL SUMMARY

The increasing reliance of systems and services on information technology in the public, private and third sector has significantly raised the impact of cyber attacks in the last two decades. The PhD programme in Security, Privacy and Trust is a response to the growing need for highly specialized training in this area. Cyber security and resiliency is a complex problem that requires understanding how business processes, cost, usability, trust and the law play a role for effective technology deployment. In addition, the right to data privacy and the need for security, transparency and auditability can at times be at odds with each other, with a balanced approach required. The UK needs well-trained specialists in all of the contributing areas, technical or otherwise, but specialists by themselves will not be enough - our future cyber security leaders will need to have a thorough understanding of the overall problem.

Our doctoral research topics will be co-created and co-developed with industry, government and non-profit partner organisations utilizing our extensive network of over 40 partners. More than 90 internship opportunities have been committed by our industry partner network allowing ample potential in terms of industry integration for all our PhD graduates. The main programme aim is to provide a comprehensive training in security, privacy and trust producing the next generation of world leading experts of the field. The emphasis is in both technical depth and ability to laterally interact with experts with different backgrounds towards collaboratively tackling the challenges in the area of security and privacy.

EDUCATIONAL AIMS OF THE PROGRAMME

The programme aims to offer the foundations for research and development for the next generation of leaders in the area of security, privacy trust. There are nine thematic areas that are covered, security analysis, programming and software security, database security and provenance, quantum security, security and privacy aspects of data mining, usability and security, security applications, and legal policy and ethics. The principal aims of the programme is to develop deep technical expertise on a specific topic of interest, ability to work with groups that have an interdisciplinary profile, ability to collaborate with industry partners, understand requirements of real world systems in terms of security and privacy, contribute to the security and privacy of deployed systems as well as the ability to reach a wider audience and educate on topics related to security privacy and trust.

PROGRAMME OUTCOMES

Knowledge and Understanding	Students successfully completing the programme will acquire a broad understanding of current topics in Security, Privacy and Trust as well as the methodology that is required to address the challenges that they pose in the real world. They will understand the breadth of the techniques available across disciplines in security and privacy and they will master technically one particular topic exhibiting an in-depth understanding of it. They will deliver significant research contributions that will be widely disseminated. They will understand responsible innovation and ethical research.

Graduate Attributes: Skills and abilities in Research and Enquiry	Graduates will have the ability to: • conduct independent research in security and privacy as well as adjacent fields • evaluate state of the art research in the field • explore alternative approaches to a given problem, and integrate different approaches • quickly assimilate existing work of relevance to a given problem
Graduate Attributes: Skills and abilities in Personal and Intellectual Autonomy	Graduates will have the ability to: • be able to assess new research ideas and turn them into research prototypes • architect and or evaluate systems from a security and privacy perspective • make use of existing work in order to make their research as relevant as possible
Graduate Attributes: Skills and abilities in Communication	Graduates will have the ability to: • communicate effectively through talks, papers, and posters • write up their research for an academic audience in the form of conference or journal papers • communicate technical content to a range of different audiences • work effectively as part of a research team
Graduate Attributes: Skills and abilities in Personal Effectiveness	Graduates will have the ability to: • acquire knowledge from a variety of sources, including the research literature, peer interaction, online materials, conferences • work effectively on large projects, both individually and as part of a team • organize their workload and manage their time when working independently, and complete complex tasks under deadline pressure
Technical/practical skills	Graduates, depending on their specific area, will have the ability to • evaluate prototypes and systems as well as develop models for arguing security and privacy properties. • use state of the art programming techniques, including cryptographic libraries • use existing data sets for their work, but also be able to collect and annotate new data • design, run, and evaluate experiments to test research hypotheses

PROGRAMME STRUCTURE AND FEATURES

MSc Phase: The MSc requires 180 credits, 140 gained through the MSc dissertation, and 40 through courses. The 40 points of courses will be chosen by the student in collaboration with the two supervisors. During the first year, all students will attend a 10 point course specific to the CDT: ``Research Methods in Security, Privacy \& Trust'' (RMiSPT). The course will have two components: The taught component of RMiSPT will synthesize all fundamental security concepts to provide students with a fast-paced introduction to the field of cyber security and privacy. The most important topics of the field will be covered following the nine thematic areas of the CDT. The aim is to expose students to the complexity and pervasiveness of problems in security, privacy and trust. As we do not expect all students to have taken an introductory course to Computer Security during their undergraduate degree, this part of the course will discuss, at a fast pace, what would be covered in such a course. The course will require twenty hours of lectures. There will be a list of fundamental topics to be covered through slides/notes prepared by the lecturer, and through a collection of research papers related to each topic. For each chosen topic, lectures will provide the background, the current state of affairs, and important techniques. In the research component of RMiSPT, the students will explore an area of interest in more depth. Each student in collaboration with their supervisors will select two research papers and, for each one, will produce a half page summary followed by four questions on its content. Students will form pairs and exchange their summaries. Each student will read the papers and attempt to answer the questions in brief also writing an assessment of the summary provided by the first student. At the end, students will prepare a presentation of one of their papers and one of the papers of their partner.

The learning objectives of the RMiSPT are as follows: the students will (1) Demonstrate a detailed understanding of some of the fundamental aspects of cyber security, privacy and trust. (2) Develop the ability to critically evaluate the literature related to their chosen topic, and to express academically-informed views on a range of security issues. (3) Demonstrate an understanding of theories and techniques for detecting and defending against a range of security and privacy threats. (4) Demonstrate ability to approach an open-ended topic, to research new ideas and experiment with new techniques. (5) Apply skills of written and oral argument within a small group setting. The course will include two one-day workshops: ``Diversity Awareness workshop'' and the ``Foundations in RRI'' course. In short, the Diversity Awareness workshop will address unconscious bias, as well as awareness of other ED\&I issues e.g., avoiding emphasis on alcohol at social events, and will inform the students about the CDT, School and University ED\&I provision, policies and processes (for more detail please see the additional ED \&I strategy document). The RRI course is described in more detail below. The remaining 30 credits will be Master's level modules across the cyber security domain, drawn from the existing graduate-level offerings in the SoI as well as suitable offerings from the other schools participating in the CDT. In this way, each student will receive a tailor-made training regime that is suitable for their focal area but will also develop a joint research perspective on cyber security.

The 140 dissertation reports on an eight-ten month research project, on a topic developed in collaboration with the assigned supervisors of the student taking into account also feedback from our industry partners. While self-contained, the project is intended to provide a strong foundation for the student's PhD thesis.

PhD Phase. The student in collaboration with their supervisors will define, structure and realise an appropriate research plan that will result in a significant advance in the area of security, privacy and trust while also incorporating feedback from our industry partners. In order to oversee progress, we will make use of the school's existing ``PhD monitoring and milestones'' framework.

Month	Year 1	Year 2	Year 3
M1	Review career aspirations and training needs	Review career aspirations and training needs	Completion strategy review
M4	Agree research area		Complete thesis outline
M6	Submit literature review	Review progress	
M9	Submit thesis proposal to supervisor	Submit a progress report and, optionally, a poster	Thesis submission
M10	Presentation to panel and feedback - 1st Year Review	Presentation to panel and feedback	Presentation to panel and feedback
M12	Supervisor completes formal first year report	Supervisor completes formal annual report	Supervisor completes formal annual report

Responsible Innovation: Responsible Research and Innovation training (RRI) will be an integral part of the training spanning both the MSc and PhD phases. In the first year, students will take the training course ``Foundations in Responsible and Innovation (RRI)'' offered www.orbit-rri.org. This one-day course covers the foundational elements of RRI including an introduction to the AREA (Anticipate, Reflect, Engage, Act) Framework. The course will be tailored to the specific research interests of each cohort. Students will suggest topics ahead of the workshop and will discuss the applicability of RRI principles to their areas of interest. During the course, students will be introduced to the Project Self-Assessment Tool which they will be encouraged to explore and revisit on a regular basis as they progress in their studies.

Entry requirements: These will be in line with the entry requirements for the existing Informatics PhD programmes:

A UK 2:1 honours degree, or its international equivalent, in computer science, mathematics, linguistics, cognitive science, or a related discipline.

All applicants must have one of the following qualifications as evidence of their English language ability:

- an undergraduate or masters degree, that was taught and assessed in English in a majority English speaking country as defined by UK Visas and Immigration
- IELTS Academic: total 6.5 with at least 6.0 in each component
- TOEFL-iBT: total 92 with at least 20 in each section
- PTE(A): total 61 with at least 56 in each of the Communicative Skills scores
- CAE and CPE: total 176 with at least 169 in each paper
- Trinity ISE: ISE II with distinctions in all four components

Progression requirements: All courses CDT students take (including individual project and group project) are assessed through exams or coursework, and a mark is awarded for each course. These marks will be ratified by the MSc Board of Examiners in Informatics. The PhD research component is evaluated through a written annual progress report that the student also presents as a talk or poster. The two supervisors of the student, together with a third faculty member, evaluate the progress report and the presentation.

Based on the course marks and the annual evaluations, the CDT progression committee decides annually on the progression of all CDT students. Students with satisfactory marks and annual evaluations will be allowed to progress to the next year, students whose marks and annual evaluation has not been satisfactory but shows potential for improvement will be allowed to progress under specific conditions (e.g., retaking courses, re-doing the progress report).

The CDT progression committee will consist of the CDT co-director, the CDT training coordinator, and two members of the Informatics Graduate School.

Exit awards: Students whose marks or annual evaluations are unsatisfactory will be asked to leave the program, with the option of being awarded a PG certificate, a PG diploma, or an MSc by Research.

Mode of study: full time

Language of study: English

TEACHING AND LEARNING METHODS AND STRATEGIES

The courses in the taught component of this degree is taught through lectures (typically around 16 lectures for a 10-point course, and around 32 lectures for a 20-point course). In most cases supporting materials, including notes, slides and sometimes video recordings of the lectures themselves, are made available to students on the web. Lecturers also direct students to recommended reading to supplement the lecture material.

Lectures are often supported by weekly scheduled tutorials, in which students in groups of 10–15 work through set tutorial exercises with the help of a tutor, and have the opportunity to seek assistance with the course material where required. Some courses are supported by scheduled laboratory sessions or supervised drop-in laboratory time, in which they are able to seek help with the practical (e.g. programming) aspects of the course material.

The group project and the individual project that is part of RMiSPT are delivered through a mixture of structured meetings and supervised sessions in which are designed to enable students to work independently on a research problem. The PhD research component of the degree is delivered by a team of two supervisors (principal and assistant supervisor) who hold regular supervision meetings with the student.

TEACHING AND LEARNING WORKLOAD

Please indicate the typical workload for a student on this programme for each year of study

Start Year	Time in scheduled teaching (%)	Time in independent study (%)	Time on placement (%)
1	30	70	0
2	20	80	0
3	10	90	0
4	0	100	0

ASSESSMENT METHODS AND STRATEGIES

For most courses, the student's achievement is assessed by academic staff via a combination of examinations and coursework assignments. (The balance is typically around 75% for the examination and 25% for coursework, with some variation between courses.) Depending on the course, examinations may be written or online, and assessed assignments may be pen-and-paper or practical programming exercises. Tutorial exercises are not usually assessed directly, but makes an important contribution to preparing students for examinations.

The group and individual projects are assessed via reports on the project work. This is assessed independently by two members of academic staff, typically in the light of a live demonstration of the project work given by the student. The markers then confer to agree on the final mark for the project.

ASSESSMENT METHOD BALANCE

Please indicate the typical assessment methods for a student on this programme for each year of study. Additionally please complete the Assessment matrix.

Start Year	Assessment by written exams (%)	Assessment by practical exams (%)	Assessment by coursework (%)
Year 1	25%	*0*	75%

Year 2	0%	*0*	0%
Year 3	0%	*0*	0%
Year 4	0%	*0*	0%

CAREER OPPORTUNITIES

The fact that the demand for security and privacy experts in industry, academia, and the public sector outstrips supply is well documented. Commercially, there is a variety of opportunities in small and large companies.

The supervisory team of the CDT is an experienced line-up of world-class researchers and educators that have collectively supervised more than 200 PhD students to completion. Graduates have gone on to positions in industry (ION Geophysical, Intel, Disney Research, Amazon, Ricoh, Samsung, NASA, Google, Microsoft, BBC, Facebook, 6point6, AimBrain, FiveAI, Deutsche Bank) as well as in leading academic institutions (UCL, Plymouth, TU Delft, Universities of Oxford, Bristol, Oldenburg, Auckland, Birmingham, Surrey, Munich, Cambridge University, Queen's University Belfast, Tsinghua University, Lancaster University and more).

OTHER ITEMS

Inhouse Distributed Ledger. The CDT will deploy a distributed ledger maintaining virtual tokens that will be used by the students and faculty to enhance the training experience and experiment with distributed ledger technology. In particular, incoming students will be given an allowance of a number of tokens that will be managed on a smartphone or desktop wallet. The distributed ledger will be run by the students themselves using a ``proof-of-stake'' underlying protocol that is extremely lightweight in terms of energy consumption. The ledger will allow installing smart contracts and interacting with them. Such interactions can be used to keep track of student contributions to various peer-to-peer training activities, such as preparation of study groups and lightning talks.

The Security Privacy and Trust Meetup. The meetup will be held weekly and will be an opportunity for all PhD students of the CDT to interact with each other, hear research updates in the form of short ``lightning'' talks as well as longer form student presentations of new and upcoming results, ``dry-runs'' of conference talks and presentations of classical or current advances in the area. The meetup will have a rotating theme and will be entirely student-run. Each semester there will be a PhD student responsible for assembling the meetup's schedule that will include 5-10 lightning talks as well as one longer form presentation. The theme of each meetup will be different and students will be encouraged to experiment with more in-depth coverage of a specific area of security, privacy and trust or covering more broadly two or more topics encouraging an interdisciplinary dialogue.

ABOUT THE PROGRAMME

ADDITIONAL REQUIREMENTS	
PRSB Accreditations (where relevant)	*Please note accreditations awarded or planned*
Admissions requirements **Before completing this section please contact a member of the Recruitment and Admissions team for further guidance.**	*To be demonstrated through certificated or experiential learning (around 100 words). English language requirements across the accepted tests should also be included.*
To be completed by R & A Team	*Please select to confirm that a member of the R & A section have consulted on the Admissions requirements.* ☐
Work experience/work based learning opportunities	*Details of organised work experience / work based learning opportunities available during the programme (if applicable)*

CONSULTATION	
Student body	--

External Review/Critical Friend	The proposal is currently subject to external peer review as part of the UKRI selection process. We will take into account any comments regarding the programme received from reviewers and during the selection interview.

ADDITIONAL DOCUMENTS	
Memorandum of Agreement (if applicable)	
Award letter (if applicable)	
DPT (please use your current template)	

APPROVAL

Programme Title:	PhD in Security, Privacy and Trust
Programme Proposer:	Prof. Aggelos Kiayias, Dr. Tiejun Ma, Dr. Kami Vaniea

STAGE 1: SCHOOL BOARD OF STUDIES REVIEW AND APPROVAL

Confirmation of approval of the proposal at the School Board of Studies should be entered below.

Date of BoS:
Convener Name:
Comment and Approval (BoS Minute): *Please provide either a link to the minutes of the Board or a copy of the relevant text from the minutes.*

STAGE 2: HEAD OF SCHOOL REVIEW AND APPROVAL

Head of School: *Please print name*
Comment and Approval:
Signature:

STAGE 3: COLLEGE CURRICULUM APPROVAL BOARD REVIEW AND OUTCOME

Date of CCAB:
Convener Name:

Stage 2 Outcome (please select as appropriate)	
Proposal approved ➧ Proceed to *New Programme Request & DPT creation*	☐
Proposal approved with conditions	☐
Proposal rejected with recommendations	☐
Proposal rejected	☐
Comment:	

DOCUMENT CHECKLIST	
Document	**Completed**
DPT	☐
Memorandum of Agreement (if applicable)	☐
Assessment Matrix	☐
Award letter (if applicable)	☐