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 Cyber Security, Privacy and Trust
UCAS Code	n/a
Relevant QAA Subject Benchmarking Group(s)	**n/a**
Postholder with overall responsibility for QA	Informatics Director of QA (currently John Longley)
Date of Production/revision	3/12/2018. Second revision 4/3/19.

[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 Cyber 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 Cyber 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. They will master one particular topic exhibiting an in-depth understanding of it. They will deliver 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

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 Cyber Security, Privacy and Trust. To oversee progress, we will make use of the School's existing ``PhD Monitoring and Milestones'' framework managed by the Informatics Graduate School.

Month	Year 1	Year 2	Year 3
M1	Review career aspirations and training needs	Review career aspirations and training needs	Completion strategy
M4	Agree research area		Complete thesis out
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 pa feedback
M12	Supervisor completes formal first year report	Supervisor completes formal annual report	Supervisor complete annual report

Responsible Innovation: Responsible Research and Innovation training (RRI) will be an integral part of the training spanning the PhD, as it is increasingly covered in elsewhere in Informatics. For example, students may have the chance to take a training course "Foundations in Responsible and Innovation (RRI)" offered by 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. Students can 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, or a related discipline.
- Desirable: a Masters degree or equivalent, in Information Security, Cyber Security or a closely related discipline.

Our own MSc in Cyber Security, Privacy and Trust is appropriate for the second requirement.

PhD selector: A dedicated PhD selector role will be established to manage applications to the programme within the School, in conjunction with the Informatics Graduate School procedures. The programme may also accept students who are co-supervised and co-funded with other Schools. If a student applies to this programme then Informatics will be the leading school and have ultimate responsibility for managing the student.

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

SPT PhD Committee: a committee comprised of supervisors of PhD students on the programme will be established to monitor progress of the programme and its special features, as well as individual students. The remit will include making strategic decisions on the management of the programme, including marketing and recruitment processes and fostering connections to industry and other sponsors. For individual students, the committee will make recommendations concerning progression and also oversee a programme for keeping contact with PhDs after they finish the programme (conducted in collaboration with

University Development and Alumni). The Chair of the PhD Committee will be a separate role (and assigned to a different person than the PhD Selector). A representative of the PhD student body will be elected to join the committee to contribute to strategic item discussions (but no matters concerning individual students or supervisors). In case of concerns about performance or behaviour of individual students or supervisors which cannot be handled by the committee, matters will be escalated within the Informatics Graduate School or with the Head of School of Informatics.

Progression requirements: PhD progress is evaluated through a written annual progress report that the student also presents as a talk and discusses to a small panel. The two supervisors of the student, together with a third faculty member, evaluate the progress report and the presentation. Students with satisfactory annual evaluations will be allowed to progress to the next year, with specific guidance and suggestions being provided by the panel. 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). This follows the standard School of Informatics and College reporting and progression procedures, managed in EUCLID. The main oversight lies with the Informatics Graduate School but the SPT PhD Committee will monitor students on this programme.

Exit awards: Students whose marks or annual evaluations are unsatisfactory will be asked to leave the program, with the option of being awarded an MPhil or MScR following the University DRPS.

Mode of study: Full-time, Part-time (subject to supervision and funding capability)

Language of study: English

TEACHING AND LEARNING METHODS AND STRATEGIES

PhD Research Training. Research training will be provided primarily by a supervisory team consisting of a minimum of two supervisors, who hold regular supervision meetings with the student. Contact time will vary according to the PhD topic and mode of research (e.g., applied technology, experimental, or theoretical) but a recommended minimum is 1-1.5hrs/week during the first year and 1 hr/week in subsequent years, or as the student and supervisor agree.

PhD supervisors take a mandatory training course (with refresher attendance at a minimum of every 5 years) as required by the University.

Suggestions and feedback. To further encourage best practice in PhD supervision and manage expectations between students and supervisors, the CSPT PhD committee may organise additional lightweight surveys and suggestions mechanisms from its students, delivered using Privacy-Preserving Technology which will optionally provide for anonymity.

Inhouse Distributed Ledger. Subject to additional funding required to set it up, the PhD programme will deploy an experimental distributed ledger maintaining virtual tokens that will be used by the students and faculty to enhance the training experience and experiment with the practical 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. Once up and running, the distributed ledger will be run by the students themselves using a modern ``proof-of-stake'' underlying protocol (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 organised events, such as preparation of study groups and lightning talks. We anticipate future similar schemes being used to record an individual's involvement in many CPD training activities.

The Security Privacy and Trust PhD Meetup. A meetup will be held weekly in conjunction with the group's seminar program. Alongside external speakers, there will be an opportunity for all PhD students of the programme (and others interested to join) 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, practice conference talks and presentations of classical or current advances in the area. Each semester there will be a PhD student responsible for helping to assemble the meetup's schedule. 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.

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	20	80	0
2	10	90	0
3	0	100	0

ASSESSMENT METHODS AND STRATEGIES

Assessment will follow the standard procedures for College and School PhD programmes, with a Literature Review and Thesis Proposal being produced in Year 1 and Progress Reports in subsequent years. Reports will be reviewed by a panel consisting of the students’ supervisors and at least one independent subject matter expert.

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. Assessment Matrix Template.xlsx

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

Year 2	10%	*0*	90%
Year 3	10%	*0*	90%

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 available to this programme consists of 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

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 (in its earlier form as a CDT MSc+PhD programme proposal) has been subject to external expert peer review as part of the UKRI selection process. We have taken into account the comments made by peer reviewers in providing this revised form of the proposal.

ADDITIONAL DOCUMENTS	
Memorandum of Agreement (if applicable)	
Award letter (if applicable)	

DPT (please use your current template)	

APPROVAL

Programme Title:	PhD in Cyber Security, Privacy and Trust
Programme Proposer:	Prof. David Aspinall, 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)	☐