Taught MSc in Security, Privacy and Trust

Myrto Arapinis David Aspinall Elham Kashefi Aggelos Kiayias
Markulf Kohlweiss Kami Vaniea Vassilis Zikas

April 23, 2018

1 Introduction

The increasing reliance of services on information technology in both the public and private sector has raised significantly the potential impact for cyber attacks in the last two decades. In 2016 alone the impact on global economy was as high as $450 Billion, according to reports from Hiscox and others,[1] while the cyber security threat has been characterised as serious as terrorism by the GCHQ.[2] At the same time, industry research firms like Gartner measure the current size of cyber security industry as $86 Billion[3] and various predictions of growth in the next 5 years estimate that the size of the industry will double at minimum.[4] Despite the dire need for highly qualified personnel, the industry is facing a serious shortage and there are projections of more than 1 million unfilled positions by 2020.[5] The above facts paint a picture that demands immediate action from universities to provide the vision and necessary training for the security experts that can meet the challenge of securing information technology services in the next five to ten years.

The MSc in Security, Privacy and Trust programme is a response to the growing need for highly specialised training in this area. Training at the postgraduate level can be an extremely effective catalyst given the lack of systematised secure engineering practices in information technology and the rapidly evolving nature of information technology services. The programme will aim to create a generation of leaders in the security and privacy sectors.

Our competitors are already offering new taught MSc programs in security and privacy; for example MSc in Software and Systems Security at University of Oxford, MSc in Information Security at Royal Holloway, MSc in Information Security at UCL, MSc in Cyber Security and Management at Warwick.

NCSC accreditation In this context, NCSC and its government partners have initiated across UK academia a degree certification programme to address the knowledge, skills and capability requirements for cyber security research and education. The vision of the UK Cyber Security Strategy 2016-21 is that: "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world." And Section 7 of the Strategy ('Develop') states that: "the UK requires more talented and qualified cyber security professionals". In particular, objective 7.1 is "to ensure the sustained supply of the best possible home-grown cyber security talent".[6]

The curriculum is carefully designed with the intention to obtain certification by the NSCS. NCSC-certified degrees help universities attract high quality students from around the world, they help employers recruit skilled staff, and they guide prospective students in making better informed choices when looking for a highly valued qualification.

[1] https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html
[2] http://www.bbc.co.uk/news/uk-41547478
[3] https://techcrunch.com/2017/08/16/global-cybersecurity-sending-to-grow-7-to-86-4bn-in-2017-says-gartner/
[4] https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
[5] http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html
[6] https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0

2 Goals and Overall Design

The School of Informatics' MSc in Security, Privacy and Trust is designed to attract students who want to establish a career as a security scientist in industry or the public sector, as well as students who want to explore the area prior to starting a PhD in the area of Cyber Security and Privacy. The MSc will teach the principles of systems security, and provide a solid foundation for pursuing a career in industry as well as academia.

The MSc programme will over the area with multi-disciplinary perspectives that relate to the security of information technology services and data collection, management and processing. The topics covered will be divided in three major themes covering core technology, social aspects and applications.

The MSc in Security, Privacy and Trust provides a directed programme akin to our MSc in CS, MSc in AI, DS, and CG programmes. It provides the following specialisations beyond the generic MSc in Informatics degree:

- A qualification branded as "Cyber Security and Privacy"
- A requirement for a dissertation project in a security or privacy related area. This is enforced, as with our MSc programmes in CS, AI, DS, and CG, by additional annotation of proposed projects as "suitable for the MSc in Security, Privacy and Trust".
- The requirement for a focus on security and privacy together with a breadth of knowledge across security and privacy areas. This is enforced by the requirement for 50 credits in the key areas of security and privacy training.

Industry teaching fellows The security group has the capability to fully resource the MSc in Security, Privacy and Trust. But for enhancing and diversifying students' education we do envisage in the future to resource some of the courses with teaching fellows from industry and public/governmental organisations.

Entry requirements Applicants are normally expected to have achieved a first-class or strong upper second-class undergraduate degree with honours (or equivalent international qualifications), as a minimum, in a related subject, such as computer science, informatics, engineering, mathematics, or physics.

Applicants whose first language is not English are usually required to provide evidence of proficiency in English at the higher level required by the University.

Learning objectives The goal of the MSc in Security, Privacy and Trust will be to teach students the major theories, best practices and essential tools for designing, implementing and evaluation secure computer systems. It will also teach students the best practices and appropriate theories and policies for the governance of cyber security in public organisations and industry. The learning objectives of the degree are to foster:

- Breadth of knowledge across the security and privacy related areas
- Advanced technical background in at least one of the security or privacy related areas
- Appreciation for real-world problems faced by industry and the public sector when it comes to security and privacy
- Research experience in one of the security and privacy related areas

The delivery of cyber security material will complement the ongoing work in the University towards distance learning offering and apprenticeships.

3 Degree Structure

The degree structure follows that of our MSc programmes in Informatics (Inf), Computer Science (CS), Artificial Intelligence (AI), Data Science (DS), and Cognitive Science (CG). The degree will consist of

- 120 credits of predominantly level 11 courses drawn from existing provision, with a minimum of 60 credits in areas pertaining to Cyber Security and Privacy.
- 60 credit project in an area pertaining to Cyber Security and Privacy.

3.1 Existing Informatics Courses

Students will be required to complete 120 credits of taught courses: we will allow up to 30 credits of Level 9/10 courses, the remaining 90 credits must be at Level 11. We will draw extensively from existing Informatics courses, but students will have the opportunity to take relevant courses in other schools as well; we include explicitly in the draft DPT below School of Law, School of Social and Political Science, and School of Molecular, Genetic, and Population Health Sciences. We will require that students take the 10 credits Research Methods in Security, Privacy & Trust course (equivalent to IRR for other programmes but with focus on security and privacy related literature) and IPP as for most of our other taught MSc programmes.

3.2 Newly Introduced Informatics Courses

- Research Methods in Security, Privacy & Trust [Myrto Arapinis]
- Advanced Topics in Cyber Security and Privacy [Vassilis Zikas]
- Security in a Quantum World [Petros Wallden]
- Introduction to Cryptanalysis [Vesselin Verlichkov]

3.3 MSc Dissertation (Informatics)

The programme includes the standard 60pt MSc thesis. Selection of dissertation topics will be handled in the same way as in our MSc in Inf, MSc in CS, MSc in AI, MSc in DS, and MSc in CG with suitable project proposals categorised as "Suitable for the MSc in Security, Privacy and Trust".

The dissertation will be due on the same date as that for the MSc in Inf, the MSc in CS, the MSc in AI, the MSc in DS, and the MSc in CG. All dissertations will be numerically marked by two markers, and moderated using the same scheme as those MSc programmes.

4 Progression, Exam Boards, and Exit Routes

The Exam Board will sit contemporaneously with that for the MSc in Inf, the MSc in CS, the MSc in AI, the MSc in DS, and the MSc in CG. Progression to dissertation, and exit to Diploma, will have the same criteria as those MSc programmes.

5 Resource Implications

The additional resources required to deliver this MSc are minimal. Indeed, the primary goal of introducing this new MSc programme is to establish a stable programme that will attract high quality students, rather than to increase the number of enrolled students beyond our planned overall MSc cohort numbers:

- **External examiner.** We will invite the current external examiners for the MSc in Inf, the MSc in CS, the MSc in AI, the MSc in DS, and the MSc in CG to also be the external examiners for this degree.
- **Course Organiser.** We propose to use the same Course Organiser as the MSc in Inf, in CS, the AI, in DS, and in CG, but will endeavour to find a staff member who will be to dealing with specialised questions about courses and course choices, much as the specialism advisers used to. The proposed mechanism will be to assign MSc in Cyber Security and Privacy students to personal tutors who have expertise in security or privacy related area - since we have a reasonable number of staff with this expertise, this should not pose any problems.
- **Project supervision.** Students on this MSc will have a rightful expectation that their project will be in an area pertaining to Cyber Security and Privacy. To ensure an adequate number of suitable security and privacy related projects, we plan to limit the intake to this degree to 25 in the first year and limit post-matriculation transfer onto the MSc in Security, Privacy and Trust

to be conditional on there being no more than 30 students enrolled in the programme at any one time. Both of these numbers will be reviewed after the first year.

6 Degree Programme table

Compulsory courses: 90 credits

INFR?????	Research Methods in Security, Privacy & Trust	S1	11	20 credits	[Myrto Arapinis]
INFR11147	IRP	S2	11	10 credits	
INFR11147	DISS	FY	11	60 credits	

Course options: 90 credits

- Select 50 to 90 credits from these options

CS Security related courses					To be proposed
INFR11131	Introduction to Modern Cryptography	S1	11	10 credits	
INFR11144	Blockchains and Distributed Ledgers	S1	11	10 credits	
INFR?????	Cryptanalysis	S1	11	10 credits	[Vesselin Velichkov]
INFR11098	Secure Programming	S2	11	10 credits	
INFR11146	IoT Systems, Security, and the Cloud	S2	11	20 credits	
INFR?????	Usable Security	S2	11	10 credits	
INFR?????	Advanced Topics in Cyber Security and Privacy	S2	11	10 credits	[Vassilis Zikas]
INFR?????	Security in a Quantum World	S2	11	10 credits	[Petros Wallden]

- Select 0 to 40 credits from these options

General CS courses				
INFR11101	Advances in Programming Languages	S1	11	10 credits
INFR11088	Extreme Computing	S1	11	10 credits
INFR11017	Human Computer Interaction	S1	11	10 credits
INFR11130	Machine Learning and Pattern Recognition	S1	11	20 credits
INFR11124	Social and Technological Networks	S1	11	10 credits
INFR11099	Introduction to Quantum Computing	S1	11	10 credits
INFR11114	Types and Semantics for Programming Languages	S1	11	10 credits
INFR11015	Applied Databases	S2	11	10 credits
INFR11120	Embedded Systems	S2	11	10 credits
INFR11023	Parallel Programming Languages and Systems	S2	11	10 credits
INFR11082	Performance Modelling	S2	11	10 credits
INFR11134	Probabilistic Modelling and Reasoning	S2	11	20 credits
INFR11038	Software Architecture, Process, and Management	S2	11	10 credits
INFR11049	Computer Networking	S2	11	10 credits
INFR11022	Distributed Systems	S2	11	10 credits
INFR11020	Algorithmic Game Theory and its Applications	S2	11	10 credits
INFR11129	Formal Verification	S2	11	10 credits
INFR11089	Randomness and Computation	S2	11	10 credits

- Select 0 to 40 credits from these options

Non-CS Security related optional courses				
LAWS11322	Practice of International Banking and the Law	FY	11	40 credits
LAWS11188	Data protection and Information Privacy	S1	11	20 credits
PGSP11467	Controversies in the the Data society	S2	11	20 credits
GLHE11055	Ethics and Governance of eHealth	S2	11	10 credits
LAWS11063	Law and New Technologies - Artificial Intelligence, Risk and the Law 2	S2	11	20 credits
LAWS11358	Contemporary issues in the Law and Policy of e-Commerce, the Digital Economy and International Information Governance	S2	11	20 credits
LAWS11231	Surveillance and Security	S2	11	20 credits
PGSP11162	International Security	S2	11	20 credits
LAWS11396	Cybercrime and Cyber Security	S2	11	20 credits

- Select 0 to 20 credits from these options
  - Select 0 to 20 credits from Level 11 courses in Schedules A to Q, T and W, as available. Notes: These are courses in all schools other than the Medicine or Veterinary Studies
  - Select 0 to 20 credits from Level 11 courses in Schedules A to Q, T and W, as available. Notes: These are courses in all schools other than the Medicine or Veterinary Studies