School of Informatics Teaching Course Proposal Form

This version was generated **May 9, 2018**. User 'marapini@inf.ed.ac.uk' verified.

Proposal

Course Name:	Research Methods in Security, Privacy & Trust
Proposer's Name:	Myrto Arapinis
Email Address:	marapini@inf.ed.ac.uk
Course Year:	

Names of any courses that this new course replaces :

Course Outline

Course Level:	11
Course Points:	20
Subject area:	Informatics
Programme Collections:	

Teaching / Assessment

Number of Lectures:	30
Number of Tutorials / Lab Sessions:	
Identified Pre-requisite Courses:	
Identified Co-requisite Courses:	
Identified Prohibited Combinations:	

Assessment Weightings:

Written Examination:	50%
Assessed Coursework:	50%
Oral Presentations:	%

Description of Nature of Assessment:

Written exam - The taught component will be examined through a written exam at the end of the semester. The exam will include questions that test Learning Objectives 1 and 3. The exam will consist of 6-8 short-answer questions each one pertaining to one of the topics discussed in lectures. The students will be required to answer 4-5 out of these questions.

Coursework - The coursework will assess the research component of the course corresponding to Learning Objectives 2 and 4. Students will be required to read papers, present papers, write essays on a topic related to one of the seed papers. More precisely, the students will deliver their work in three instalments:

- one review of one of the seed papers in the spirit of conference reviewing. The student will take the role of a member of the programme committee of the conference and provide a critical evaluation of the paper.

- one oral presentation of one of the seed papers. The student will present the paper as he was one of the authors presenting it to the accepted conference.

- one essay on a topic related to one of the seed papers - summary of the paper, and analysis of (critical thoughts on) the paper. This is the replacement of the IRR.

Course Details

Brief Course Description:

This is a proposal for a new course. The course will cover advanced topics in Cyber Security, Privacy, and Trust. The course aims to develop a deep understanding of current computer security and privacy research. By exposing students to current research and developments in connection with Cyber Security, Privacy and Trust, the course will prepare them for conducting research in this area.

The course is intended to be offered to students on the MSc in Security, Privacy and Trust programme. This will be a mandatory course for those students, and will have two components:

1. Taught component - Synthesize the fundamental security concepts to provide students with a fast-paced introduction to the field of cyber security and privacy. The most important topics will be covered in this part including Network security, Usable security, Cryptography, Cryptographic protocols, OS security, Malware, Web security. The aim is to expose students to the complexity and pervasiveness of the security problem, and how this presents challenges. As we do not expect all students to have taken a introductory course to Computer Security in their undergraduate, this part of the course will discuss at a fast pace what would be covered in such a course.

2. Research component - Students will explore an area of interest in more depth than allowed in standard taught courses very much like the IRR on the other Informatics' MSc programme.

We would expect students 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 (as for the MSc in Security, Privacy and Trust).

The proposed name for the course is Research Methods in Security, Privacy & Trust (RMiSPT). It will focus on the main aspects of Cyber Security, Privacy, and Trust: Cryptography, Software vulnerabilities, Web security, Access control, Mobile security, Differential privacy, Hardware protection, Side channel attacks, Blockchain, Network security, Usable security, Passwords, etc.

The course will require an allocation of an equivalent of 20-30 one-hour lecture slots in total. 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 affair, and important techniques. The taught component will be complemented by a seminar like research component for which students will be required to read, evaluate and present recent papers from the top conferences in the area. This part of the course will be run like an academic conference: students will in turn act as members of the conference Programme Committee, and scientific contributor to the conference.

The course will target MSc students on the MSc in Security, Privacy, and Trust. Due to the format of the course, there is a natural cap on the number of students that can be enrolled in the course. Each one-hour session will host two students presentations, so the maximum capacity for this course is 30-35 students.

Given the theory nature of the course, no computing resources will be required. The course lecturer(s) will point to current research work. There will be need for standard teaching support in the form of a teaching assistant to help inshaping up the various topics chosen by the student, potentially answering some of their questions during the development phase of their projects, and marking essays.

Detailed list of Learning Objectives:

1: Demonstrate detailed understanding of some of the fundamental aspects of cyber security, privacy and trust

2: Develop ability to critically evaluate the literature related to their chosen topic, and to formulate 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. The course emphasises on the technical material

4: Demonstrate ability to approach an open-ended topic, to research new ideas and experiment with new techniques. Complete a project that contributes in an original way to an established area of research or development

5: Developed skills of written and oral argument within a small group setting. Write a project according to a standard that would be acceptable for wider publication. Report and present the project. The oral presentation should accurately summarise their work

Syllabus Information:

TBD

Recommended Reading List:

List of seed research papers provided by the lecturer

Any additional case for support information:

To be either a professional or a researcher in the area, it is necessary to understand fundamental issues in connection with cyber security and privacy. The course will fill a gap in the current curriculum. While several courses are related to security and privacy, none of the courses offers a comprehensive coverage of fundamental challenges in the field.

There is a strong push from central government for research and teaching in Cyber Security, as part of the national UK Cyber Security Strategy. This course is part of our submission for a dedicated MSc programme which could be popular, but this requires new courses such as this one.

Also, we have been accreditated by GCHQ/EPSRC as Academic Centre of Excellence in Cyber Security Research. This will very probably drive students with interest in Cyber Security and Privacy to us, but we would need courses as the proposed one for them.