School of Informatics Teaching Course Proposal Form

This version was generated **April 30, 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: 0
Identified Pre-requisite Courses:
Identified Co-requisite Courses:
Identified Prohibited Combinations:

Assessment Weightings:
Written Examination: 0%
Assessed Coursework: 60%
Oral Presentations: 40%

Description of Nature of Assessment:

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 three 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 accreditation 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.

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 - Introduce the fundamental security concepts and offer a working knowledge of threats and counter-measures. The topics covered will include Network security, Usable security, Cryptography, Cryptographic protocols, OS security, Malware, Web security. We do not expect all students to have taken a introductory course to Computer Security in their undergraduate. This part of the course will cover 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 (MSPT). 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 conferencesin 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.

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:

In keeping the seminar nature of the course, there will be no exams. The evaluation scheme for courses like ATFD works much better with this type of courses. Students will be required to read papers, present papers, write essays on a topic related to one of the seed papers, and complete a small project. More precisely, the students will deliver their work in three instalments:

1: one oral presentation of one of the seed papers

2: one essay on a topic related to one of the seed papers - summary of the paper, and analysis of (critical thoughts on) the paper

3: a small project related to one of the seed papers, add a new contribution done by the student to the selected paper. This could be

- An implementation of a theoretical algorithm with performance analysis
- An extension of some of the results to cover new cases
- An improvement for an existing solution, perhaps under some restrictions
- etc. (the list is not exhaustive)