Security Testing for Cyber-Physical Systems

Highlights

- Development of methods and tools for testing of Cyber-Physical Systems against cyber- and physical-security attacks
- Building of public trust in the resilience of autonomous vehicles against cyber-crime
- Potential impact on government policies in defence and security

Overview

As self-driving cars turn from a dream into a reality, and as our lives become increasingly dependent on software-controlled medical devices such as, for example, pacemakers and insulin pumps, guaranteeing the security of such Cyber-Physical Systems (CPS) and their robustness against hacker attacks becomes of paramount importance. Notable examples of such attacks include the disruption of a vehicle breaking system by injecting faulty sensor data, or compromising the function of an insulin delivery device.

The rigorous development of such life-critical systems using mathematical models and sound methods for their analysis can greatly improve manufacturers’ ability to build public trust in the systems’ resilience to cyber-crime. Due to this, the security-aware modelling and design of CPS has recently become an important research topic in computer science. Since such systems include complex interactions between physical and cyber components, they are susceptible to a much wider range of attacks than traditional software systems. This requires the development of appropriate formalisms for describing such attacks in a precise way, and methods for providing a certain degree of confidence in their security against such attacks.

The goal of this project is to address these challenges by developing methods for the testing of CPS against formally specified security requirements. By identifying security vulnerabilities through testing and eliminating them through system re-design, the resulting methodology for CPS development will be able to provide a level of confidence in the final product. By building upon and extending formalisms for the specification of security properties and established notions for conformance testing of CPS, this research will provide novel methods and tools for rigorous security-aware development of CPS.

The developed techniques will be evaluated on case-studies in the domains of autonomous vehicles and medical devices. The research outcomes will be of interest for national and international defence and security labs.
Methodology

The research undertaken in this project will build upon the expertise of the two supervisors in the areas of (1) cyber and physical security (analysing information flow in software systems, and designing surveillance strategies for mobile sensors) and (2) conformance testing for CPS (testing the conformance of a CPS against a test model).

We envision that the conformance relations used in conformance testing will play a crucial role in extending specification formalisms for cyber-security properties to the physical world. Existing testing techniques will have to be extended to this new class of properties, and the key challenge will be to formally establish what guarantees these novel methods will be able to provide.

The student will have the opportunity to work in a department with strong research traditions in Software Engineering and Formal Methods, on a highly relevant and very timely topic.

Further Reading

**Specification of security properties in temporal logics (by first supervisor)**

1. Rayna Dimitrova, Bernd Finkbeiner, Máté Kovács, Markus N. Rabe and Helmut Seid. Model Checking Information Flow in Reactive Systems. (VMCAI 2012)

**Conformance testing of CPS (by second supervisor)**


Funding

This research project is one of a number of projects in the Department. It is in competition for funding with one or more of these projects. Usually the project which receives the best applicant will be awarded the funding.

**Home/EU Applicants**

This project is eligible for a fully funded College of Science and Engineering studentship which includes:

- A full UK/EU fee waiver for 3.5 years
- An annual tax free stipend of £14,777 (2018/19)
- Research Training Support Grant (RTSG)
International Applicants
This project is eligible for a fully funded College of Science and Engineering studentship which includes:

- A full international fee waiver for 3.5 years
- Research Training Support Grant (RTSG)

Application Instructions
The online application and supporting documents are due by Monday 21st January 2019.

Any applications submitted after the deadline will not be accepted for the studentship scheme.

References should arrive no later than Monday 28th January 2019.

Applicants are advised to apply well in advance of the deadline, so that we can let you know if anything is missing from your application.

Required Materials
1. Online application form
2. Two academic references
3. Transcripts
4. Degree certificate/s (if awarded)
5. Curriculum Vitae
6. CSE Studentship Form
7. English language qualification

Applications which are not complete by the deadline will not be considered for the studentship scheme. It is the responsibility of the applicant to ensure the application form and documents are received by the relevant deadlines.

All applications must be submitted online, along with the supporting documents as per the instructions on the website.

Please ensure that all email addresses, for yourself and your referees, are correct on the application form.

For more information, please visit our website at:
https://www2.le.ac.uk/colleges/scieng/research/postgraduate-opportunities/cse-2019/instructions