Postgraduate Studentships Queen's Doctoral Training Programme on Secure Connected Intelligent Design and Manufacturing

School of Electronics, Electrical Engineering and Computer Science

PhD Studentship 2020/21

Proposed Project Title: DTP: Making STRIDES in Cyber Physical System Security: Improving Threat Analysis for Industry 4.0

Principal Supervisor:
Dr Kieran McLaughlin

Contact Details:
QUB Address ECIT Institute,
Centre for Secure Information Technologies (CSIT)
Tele No: 028 9087 1890
E-Mail: kieran.mclaughlin@qub.ac.uk

Research Area

Cyber Security / CSIT _____

Proposal open to other School **(indicate area of Interest)**

MAE (this topic is not necessarily restricted to CS/ELE domain experts)

_____

Degree linked to ELE

This project is part of the Queen's Doctoral Training Programme in Secure Connected Intelligent Design and Manufacturing. Many of today's industrial approaches require transformative changes to ensure long term societal, economic and environmental resilience and sustainability. PhD projects in this programme explore the potential of emerging digital technologies, such as artificial intelligence, robotics, and the Internet of Things, to transform the way we design, manufacture and operate products and services.

The programme offers a bespoke research and training programme that aims to develop students into cross-disciplinary, industry-conscious thinkers and leaders who will influence the roadmaps of future advanced manufacturing technologies and their applications. They will have a balanced understanding of ICT (security, communications and data analytics) in the context of their application to Advanced Manufacturing and High Value Design.

Project Description:

Cyber-Physical Systems (CPS) comprise interacting IT and physical components. CPS includes emerging new technologies such as the Internet of Things (IoT), industrial systems, and "smart" technologies related Industry 4.0. Understanding cyber security for CPS is a significant challenge, due to the cyber and physical aspects of these systems which are interdependent and constantly interacting.

The Biohaviour project [1] at QUB for example, seeks to develop a cloud-connected, design-manufacturing enterprise inspired by nature. Here, a digital design model (CAD) adapts based on live feedback from the physical manufacturing system, end customers and supply chain. Signals back and forth between different elements of the enterprise are treated as "Stimuli" to which the design "Growth" responds. The vision is that better performing, more efficient products will ultimately emerge. However, the connected nature of the system gives rise to potential vulnerabilities and cyber threats.

STRIDE is an approach used to systematically identify cyber threats (i.e. Spoofing, Tampering, Repudiation, Information disclosure, DoS, Elevation of privilege) against a particular IT system. STRIDE was developed with a data-centric viewpoint, focussed primarily on software security. It is generally a high-level analytical approach, such that it normally does not explore deeper details such as individual component vulnerabilities or exploits. Nonetheless, compared to some threat modelling approaches, STRIDE is attractive for its conceptual simplicity and approachability for users.

Part of the STRIDE process involves the development of a Data Flow Diagram (DFD) to represent the components and data associated with the system being analysed. From the perspective of a CPS, the DFD approach is attractive, as it potentially offers scope to capture physical and manufacturing attributes (physical components, environmental attributes and data flows), in addition to the conventional IT aspects.

To enable applicability to CPS, research is therefore necessary to re-evaluate the coverage of STRIDE, to encompass physical components, interactions, sensor measurements, and so on, which can be affected by cyber-attacks against a CPS. Furthermore, research is required to investigate how detailed device and process level vulnerabilities can be incorporated into the new threat analysis approach to support more meaningful threat responses.

Objectives:

- Investigate and analyse current threat-centric analysis frameworks, including STRIDE, PASTA, and HAZOP approaches [2], [3].
- Analyse the six STRIDE elements to evaluate their coverage and suitability to model physical domain aspects of a CPS. Explore how techniques that focus on physical safety constraints and hazop conditions are defined, and consequently propose new elements for STRIDE that allow it to capture threats across the cyber and physical components, particularly of modern manufacturing plants and infrastructure.
- Further research steps should focus on deeper analysis of emerging concerns for threat analysis as new technologies are integrated into CPS. This challenge includes questions about how to capture the possible threat of machine learning or AI, where unanticipated threats may be realised due to autonomous decision-making algorithms driving a system or components into unforeseen states or sequences of behaviour that threaten safety or security.
- Develop and explore use-case scenarios to demonstrate the effectiveness of the new proposals to improve STRIDE.

[1] http://www.biohaviour.com

[2] https://ieeexplore.ieee.org/abstract/document/8260283

[3] https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Academic Requirements:

A minimum 2.1 honours degree or equivalent in Computer Science or Electrical and Electronic Engineering or relevant degree is required.

GENERAL INFORMATION

This 3.5 year PhD studentship, potentially funded by the Department for Employment and Learning (DfE), commences on 1 October 2020.

Eligibility for both fees and maintenance (approximately £15,000) depends on the applicants being either an ordinary UK resident or those EU residents who have lived permanently in the UK for the 3 years immediately preceding the start of the studentship. Non UK residents who hold EU residency may also apply but if successful may receive fees only.

Applicants should apply electronically through the Queen's online application portal at: https://dap.qub.ac.uk/portal/

Further information available at: https://www.qub.ac.uk/schools/eeecs/Research/PhDStudy/

Closing date for applications: 15 March 2020