Information on Postgraduate Research Scholarship - Ref: VCS-FES-03-25			
Faculty:	Engineering & Science	**Department:**	Centre for Sustainable Cyber Security
Lead Supervisor:	Dr. M. Taimoor Khan		
Project Title:	Resilient-by-design Cyber Physical Systems against Data Integrity Attacks		
Project Description:	Modern cyber-physical systems (CPS), such as UAVs, next-generation fighter aircraft, and command-and-control (C2) platforms, integrate digital computation with physical processes to make mission-critical decisions in real time. These systems rely heavily on sensor data (e.g., GPS, pressure transducers, image processors), making them vulnerable to stealthy threats like False Data Injection (FDI) and sensor spoofing. These attacks manipulate input data while maintaining apparent operational normality, potentially leading to unsafe decisions without detection. This project aims to develop a novel verification methodology and corresponding toolchain to detect and mitigate such threats to CPS at the design time making the CPS resilient-by-design. Typically, CPS are modelled as hybrid systems, comprising discrete (cyber) and continuous (physical) components. The core technical innovation lies in modelling the verification problem as a delta-decision problem, solved using an extended SMT (Satisfiability Modulo Theories) solver. The work aims to demonstrate methodology through the application of the prototype to a real-world industrial system (provided by our industrial partner - Evolution Measurement) that is used in flight test environment and is a true representative of a defence C2 system. Specifically, the project aims to test C2 operations that involve differential pressure scanner (e.g., P10-D) by estimating physical state for FDI vulnerabilities through modelling the system and evaluating the provided aerodynamics flight data by comparing the consistency between real-time “observations” (i.e., extracted from the collected data) and “predications” (generated by the C2 operational model). The tool will detect subtle discrepancies indicative of stealthy data manipulation with zero false alarms, outperforming conventional static, dynamic and AI-based techniques. Specifically, in case of any inconsistency, the tool produces a counter example with values that constitute the vulnerability. Such pressure sensors are widely used in C2 defence systems, e.g., missile and aircraft testing, battlefield environmental monitoring, and UAV and autonomous system applications, to name a few. Candidates for this PhD should have a strong foundation in computer science and mathematical modelling/logic, along with proven skills in prototyping software for critical/serious applications. If you have any questions, you can contact Dr. M. Taimoor Khan, Email: m.khan@greenwich.ac.uk		

June 2025

	Note that the University of Greenwich with its Centre for Sustainable Cyber Security (CS2) of with 50+ researchers and PhD students, the Centre for Sustainable Cyber Security (CS2) has been conducting pioneering research across several areas of cyber security, from trustworthy IoT, to certified cyber physical system security and protection against disinformation in social media. Thanks to these successes, the university is now one of only nine in the UK recognised as Academic Centre of Excellence for Cyber Security in both Research and Education (ACS-CSR, ACS-CSE). The successful candidate will actively collaborate with industrial partner (Evolution Measurement) and will have the opportunity to work with NCSC and in a vibrant research environment in CS2.
Duration:	3 years, Full-Time Study

Bursary available (subject to satisfactory performance):

Year 1: £20,780 (FT) or pro-rata (PT) Year 2: In line with UKRI rate Year 3: In line with UKRI rate

In addition, the successful candidate will receive a contribution to tuition fees equivalent to the university's Home rate, currently £5,006 (FT) or pro-rata (PT), for the duration of their scholarship. International applicants will need to pay the remainder tuition fee for the duration of their scholarship.

This fee is subject to an annual increase.

Person Specification of Essential (E) or Desirable (D) requirements:

Criteria:	**E or D**
Education and Training:	
• 2:1 (UK or UK equivalent) in computer science, engineering, mathematics or related areas, or a master's degree with 60% overall in a relevant discipline.	**E**
• For those whose first language is not English and/or if from a country where English is not the majority spoken language (as recognised by the UKBA), a language proficiency score of at least IELTS 6.5 (in all elements of the test) or an equivalent UK VISA and Immigration secure English Language Test is required, if your programme falls within the faculty of Engineering and Science a language proficiency score of at least IELTS 6.5 overall with a minimum of 6.0 in all elements of the test or an equivalent UK VISA and Immigration secure English Language Test is required. Unless the degree above was taught in English **and** obtained in a majority English speaking country, e.g. UK, USA, Australia, New Zealand, etc, as recognised by the UKBA.	**E**
Experience & Skills:	
• Previous experience of undertaking research (e.g. undergraduate or taught master's dissertation)	**E**
• Excellent software development skills	**E**
• Experience in mathematical modelling or logic	**D**
• Demonstrable interest in vulnerability analysis or cyber security	**D**
• Demonstrable interest in cyber physical systems or aerodynamics	**D**

• Excellent organisational and IT communication skills	**D**
Personal Attributes:	
• Understands the fundamental differences between a taught degree and a research degree in terms of approach and personal discipline/motivation	**E**
• Able to, under guidance, complete independent work successfully	**E**
• Excellent time and project management skills	**E**
Other Requirements:	
• This scholarship may require Academic Technology Approval Scheme approval for the successful candidate if from outside of the EU/EEA	**E**
• The scholarship must commence by **October *2025***	**E**
Closing date for applications:	***midnight UTC on 5th September 2025***
For further information contact:	Dr. M Taimoor Khan, Email: m.khan@greenwich.ac.uk

Making an application:

Please read this information before making an application. Information on the application process is available at: https://www.gre.ac.uk/research/study/apply/application-process. Applications need to be made online via this link. **No other form of application will be considered**.

All applications **must include** the following information. **Applications not containing these documents will not be considered.**

- **Scholarship Reference Number (VCS-FES-03-25)**– included in the personal statement section together with your personal statement as to why you are applying. The REF is "VCS-FES-03-25"
- **CV***
- **Academic qualification certificates/transcripts and IELTs/English Language certificate -** if you are an international applicant or if English is not your first language or you are from a country where English is not the majority spoken language as defined by the UK Border Agency *
- **Personal Statement -** outlining your motivation for applying for this PhD, and your previous research experience (e.g., as a research assistant or completing a dissertation).
- **Research Proposal** (ca. 2000 words) – A literature review on detecting data integrity (e.g., false data injection) attacks in cyber physical systems and your ideas on how this project can be conducted.
- **Examples of relevant software** prototypes or code repositories (e.g., GitHub) demonstrating experience with vulnerability analysis, cyber security applications, cyber physical systems, formal methods or mathematical modelling/logic implementations.

**upload to the qualification section of the application form. Attachments must be a PDF format.*