THE UNIVERSITY OF MANCHESTER

PARTICULARS OF APPOINTMENT

FACULTY OF SCIENCE & ENGINEERING

SCHOOL OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

RESEARCH ASSOCIATE IN FORMAL ANALYSIS OF SECURE HARDWARE (2 posts available)

VACANCY REF: S&E-015607

Salary:	£32,816 to £40,322 per annum (depending on experience)
Hours:	Full time
Duration:	Starting as soon as possible for 36 months
Location:	Oxford Road, Manchester

Enquiries about the vacancy, shortlisting and interviews:
Name: Dr Giles Reger

Email: giles.reger@manchester.ac.uk

BACKGROUND

You will be joining the *Secure Code for Capability Hardware* project (https://scorch-project.github.io/) which is one of nine projects funded under the Digital Security by Design challenge. The challenge was set up to fund research building on the capability hardware Morello platform developed by Arm.

The aim of SCorCH is to leverage and extend existing formal analysis techniques to find (and fix) security issues in software running on capability hardware (e.g. Morello). Capability hardware can be used to circumvent many normal memory safety issues and to implement advanced compartmentalisation approaches. However, security is only achieved if these features are used correctly - common issues may be fixed but this may just move the attack surface somewhere else.

Manchester has a long and distinguished track record in the research and teaching of core Computer Science, and across interfaces to adjacent disciplines. Founded upon the pioneering work of Williams, Kilburn and Turing, the School was the first academic Department of Computer Science in the UK and one of the first to run an undergraduate programme. The research strength of the school is reflected in consistently strong returns in UK research assessment exercises (5* in RAE 2000, 2nd in Research

Power in RAE 2008, 4th in overall GPA in REF 2014 and ranked equal 1st for research environment). The Formal Methods Group has a broad span of interests, ranging from developing the new mathematics of computational behaviour, through the study and development of system design and verification methods, to all aspects of logic.

SCorCH has two industrial partners. We will be working closely with Arm to ensure that the SCorCH solution aligns with ongoing developments on the Morello platform. We will be working closely with Automated Reasoning Group at Amazon Web Services to explore real-world applications of the SCorCH solution.

Overall Purpose of the Role

The SCorCH approach will follow three main verticals of exploration - Bounded Model Checking, Runtime Verification, and Automated Reasoning. Each position will work within **one** of these verticals but will be expected to work closely with the other verticals. These two positions should work in either the Runtime Verification or the Automated Reasoning vertical. Context on each vertical is provided below.

We will extend bounded model checking techniques and tools (e.g. CBMC and/or ESBMC) with new operational models reflecting the Morello architecture, new analyses for the modified notion of memory safety and compartmentalisation requirements, and further extensions to improve their applicability in the industrial context.

We will utilise runtime verification (a dynamic analysis) to detect security issues at runtime. Behaviour will be intercepted at different levels of the software stack and instruments inserted to track necessary information. We will further explore approaches leveraging partial information from model checking analysis, integrating dynamic symbolic execution based fuzzing techniques, and utilising specification inference/learning techniques to identify new temporal properties to be monitored.

We will extend automated reasoning tools (e.g. Vampire or iProver) to support new theories enabling them to reason effectively about proof obligations related to capabilities. We will target the proof obligations produced by bounded model checking, symbolic execution, hardware model checking, and security proofs in proof assistants. We may also explore new techniques for hardware model checking or extend the set of security properties established within proof assistants.

Key Responsibilities, Accountabilities or Duties:

The range of duties will include:

- Development of new theory and methodologies
- Implementation of new techniques in industrial-strength tools
- Writing scientific articles based on the research results
- Attending national and international meetings to present research results
- Visit industrial partners and work closely with them
- Collaborate with colleagues internationally
- Work independently when required
- Plan and manage own research activity in collaboration with others.

There may be opportunities for the applicant to be involved in either teaching or supervision related activities as appropriate and in agreement with the line manager.

PERSON SPECIFICATION

Essential Knowledge, Skills and Experience*:*

- Have, or be about to obtain, a PhD or equivalent in a relevant area
- Excellent knowledge in at least one of the following areas
    - Bounded Model Checking
    - Runtime Verification
    - Dynamic Symbolic Execution/Abstract Interpretation
    - Automated Reasoning/First-order Theorem Proving
- Strong coding skills
- Excellent communication and interpersonal skills
- Ability and willingness to work closely with industry
- Ability to work independently and as part of a team
- Ability to present in both written and oral publications

Desirable:

- A track-record of high-quality publications
- Previous implementation experience with a formal analysis tool
- Knowledge and experience of hardware design
- (For third vertical) Knowledge and experience of proof assistants, e.g. Isabelle or HOL