VeTSS RESEARCH INSTITUTE IN

VERIFIED TRUSTWORTHY SOFTWARE SYSTEMS

Verified Software Workshop
24-25 September 2019

Isaac Newton Institute for Mathematical Sciences, Cambridge

Programme

Morning of Tuesday, 24th September 2019

09:00-09:25 Registration with Tea and Coffee

09:25-09:30 Welcome by **Philippa Gardner** (Imperial College London, Director of VeTSS) and **Christie Marr,** (Deputy Director, Isaac Newton Institute for Mathematical Sciences).

09:30-10:15 **Andreas Rossberg (Dfinity Foundation, USA and Germany)**

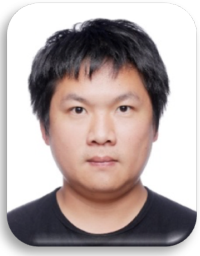
Language Formalisation Goes Mainstream

WebAssembly (a.k.a. Wasm) is a new low-level virtual machine originally designed for the Web and available in all modern browsers. It has already spread to various other environments, such as cloud and edge computing, sandboxing, mobile, or embedded. Rather than committing to a specific programming model, it is an abstraction over modern hardware, making it both language- and platform-independent. Wasm is the first industrial language technology that has been designed, defined, and standardised with a complete formal specification at the centre, drawing from decades of research and established practices in academic work.

Andreas Rossberg is a staff researcher with the Dfinity Foundation. Before that he was a software engineer at Google, where he worked on V8, the JavaScript virtual machine. Prior to his move to industry, he was a researcher at the Max Planck Institute for Software Systems after receiving a PhD from Saarland University. He is one of the main designers of WebAssembly, authored its formalisation and specification, and is the champion of various proposals for enhancements. At Dfinity, he is working on employing WebAssembly for decentralised cloud computing. His research interests revolve around programming languages, ranging from foundational theory and design to implementation techniques.

10:15-11:00 **Ming Fu,** (Huawei)

Taking Formal Verification of Systems Software from Academia to Industry



Formal verification of systems software (e.g., operating systems and file systems) has recently received widespread attention in both academia and industry. In this regard, the OS Kernel Lab at Huawei has independently developed a microkernel-based operating system, where we have applied formal verification techniques to build a reliable, secure kernel. In this talk, I will first share our experience in applying the formal verification techniques from academia to industry in the context of the microkernel project. Furthermore, I will present our on-going efforts on applying refinement-based verification techniques to successfully verify a concurrent file system called AtomFS.

Dr. Ming Fu is the President of the Huawei Dresden Research Center. He joined Huawei two years ago and led the formal verification team to formally verify the microkernel developed by Huawei OS kernel lab. He was an associate professor in the University of Science and Technology of China (USTC) before joining Huawei. His research interests include concurrency verification, refinement-based verification, and OS kernel verification. He led the verification group in USTC to verify the commercial real-time embedded kernel uC/OS-II in Coq.

11:00-11:30 Tea and Coffee break

11:30-12:15 **Peter Sewell,** (Cambridge University, UK)

Fixing the Foundations with Semantics and Capabilites: ARM, RISC-V, and CHERI

Any software verification has to build on an underlying semantics, which ultimately has to be that of the architecture: the envelope of allowed processor behaviour that correct hardware implementations must lie within, and that software must assume. For a small idealised architecture, this is straightforward, but precisely defining an industrial or production-scale research architecture raises many interesting challenges, both technical and social/engineering. Focussing mostly on sequential instruction-set semantics, this talk will look at the state of the art, first for Arm, where we have semantics for the full ARMv8-A architecture, automatically translated from the Arm-internal reference, and for RISC-V, with a semantics being adopted by the RISC-V Foundation. The talk will continue with the CHERI architecture, enabling fine-grain memory protection and secure encapsulation, while offering a smooth upgrade path for existing software, using novel hardware support for capabilities. CHERI uses a range of rigorous engineering techniques to speed development and increase assurance, in a hardware/software/semantics co-design process. Instruction-set semantics is at the heart of CHERI design and engineering, both in lightweight ways that support and improve normal engineering practice - as documentation, in emulators used as a test oracle for hardware and for running software, and for test generation - and for formal verification. We formalise key intended security properties of the ISA specifications, and establish that these hold with mechanised proof. CHERI underpins the ISCF Digital Security by Design programme, and this talk will also touch on the formal artifacts that we expect to make available for that - with systems aspects covered in the later talk by Robert Watson.

Peter Sewell is a Professor of Computer Science at the University of Cambridge Computer Laboratory. He held an EPSRC Leadership Fellowship from 2010-2014 and a Royal Society University Research Fellowship from 1999-2007; he took his PhD in Edinburgh in 1995, supervised by Robin Milner, after studying in Cambridge and Oxford. His research aims to build rigorous foundations for the engineering of real-world computer systems, to make them better-understood, more robust, and more secure. He and his colleagues have recently focussed on the relaxed-memory concurrency models of multiprocessors and concurrent languages (x86, ARM, IBM Power, and C/C++11), on verified compilation of concurrency (CompCertTSO and the concurrency compilation schemes from C/C++11 to x86, Power, and ARM), and on tools for applied semantics.

12:15-12:30 **Robert Watson** (Cambridge, UK)

Technology Transition for CHERI - Opportunities for Research

Capability Hardware Enhanced RISC Instructions (CHERI) is a novel computer-architecture extension supporting fine-grained memory protection and scalable software compartmentalization for C/C++-language Trusted Computing Bases (TCBs). The CHERI architecture project has now been running for nine years, starting life on the 64-bit MIPS ISA, and now being elaborated on multiple other contemporary mainstream ISAs. In this talk will briefly describe the CHERI architecture, and then explore technology-transition opportunities arising for CHERI as a result of the UKRI ISCF Digital Security by Design programme, identifying arising areas of future broader industrial and academic research.

Robert is a Senior Lecturer in Systems, Security, and Architecture at the University of Cambridge Computer Laboratory and has been a joint Principal Investigator for the CHERI Architecture Project over the last nine years. He is involved in several research groups at the lab, including Security, Networks and Operating Systems, and Computer Architecture and leads a number of cross-layer research projects spanning computer architecture, compilers, program analysis, program transformation, operating systems, networking, and security.

12:30-13:00 **Lightning talks**

Short talks for PhD students, RAs, academics, industrialists, and government employees to introduce themselves to each other and the audience.

13:00-14:00 Lunch and Poster session

Afternoon of Tuesday, 24th September 2019

14:00-14:45 **Jim Woodcock**, (University of York, UK)

Verification Challenges

We review Tony Hoare's verification challenges. We start in 2003 with his challenges to construct a verifying compiler and his continuing theme on unifying theories in computer science. We describe the industrial-scale pilot projects proposed to drive this challenge forward: the Mondex smart card, the space-flight flash filestore, radio spectrum auctions, the Microsoft hypervisor, NSA's Tokeneer identification station, Wittenstein's FreeRTOS real-time kernel, and Boston Scientific's cardiac pacemaker. We discuss the wider impact of the verification challenge and the sea-change since 2003. Finally, we look forward to the next 15 years and suggest a pilot project in robotics for the verification community.

Jim is Professor of Software Engineering at the University of York. He has worked closely with industry, including GEC/Marconi, IBM (Queen's Award), CESG, and British Energy, as well as many SMEs. His research interests include semantics, model checking, and theorem proving; robotics and cyber-physical systems; industrial applications and technology transfer. He is a Fellow of the Royal Academy of Engineering and Editor in Chief of the Springer journal Formal Aspects of Computing. He is the chair of the Formal Methods Europe Awards Committee. He has had long-term collaborations with colleagues in the Global South.

14:45-15:30 **Future Challenges Discussion:** Tony Hoare (University of Oxford), John Goodacre (Innovate UK) and Philippa Gardner (Imperial College London)

15:30-16:00 Tea and Coffee break

16:00-16:45 **Daniel Zimmerman**, (Galois, USA)

High Assurance Cryptography and Verifiable Elections

Dr. Daniel Zimmerman is a Principal Researcher at Galois and a co-founder of Free & Fair. He has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. Before joining Galois and Free & Fair, Dr. Zimmerman was a Visiting Associate Professor of Computer Science at Harvey Mudd College in Claremont, California. Prior to that, he was an Assistant Professor of Computer Science and Systems at the University of Washington Tacoma. He has also held both teaching and research positions at the California Institute of Technology, from which he obtained his Ph.D. in 2002. Since joining Galois and Free & Fair, Dr. Zimmerman has worked primarily in the areas of rigorous software and hardware engineering and verifiable elections technology.

16:45-17:30 **Peter W O'Hearn**, (Facebook and University College London, UK)

Incorrectness Logic

Program correctness and incorrectness are two sides of the same coin. As a programmer, even if you would like to have correctness, you might find yourself spending most of your time reasoning about incorrectness. This includes informal reasoning that people do while looking at or thinking about their code, as well as that supported by automated testing and static analysis tools. This talk describes a simple logic for program incorrectness which is, in a sense, the other side of the coin to Hoare's logic of correctness.

Peter is a research scientist at Facebook and a professor of computer science at University College London. His research has stretched from abstract topics such as category-theoretic models and logics through to logics of programs and on to automated analysis of industrial software in the millions of lines of code and its deployment to products used regularly by billions of people. As an academic, Peter worked on theories such as Separation Logic, Bunched Logic and denotational semantics. Then, after over 20 years as an academic, he took a position at Facebook in 2013 with the acquisition of a startup he cofounded, Monoidics Ltd. The Infer program analyzer, developed by Peter's team, has resulted in over a hundred thousand issues being fixed by Facebook engineers before they reach production. Peter has received a number of awards for his work, including 2011 and 2019 POPL Influential Paper Awards, the 2016 CAV Award and the 2016 Gödel Prize. He is a Fellow of the Royal Society, a Fellow of the Royal Academy of Engineering, and has received an honorary doctorate from Dalhousie University in 2018.

17:30-18:30 **Lightning talks**

Short talks for PhD students, RAs, academics, industrialists, and government employees to introduce themselves to each other and the audience.

19:30-22:00 Workshop dinner at Westminster College Hall

Westminster College Hall is on Madingley Road, Cambridge, CB3 0AA, a short walk from the Isaac Newton Institute.

Morning of Wednesday, 25th September 2019

09:00-09:45 Tea and Coffee

09:45-10:30 **Marta Kwiatkowska**, (Oxford University)

Safety verification for deep neural networks with provable guarantees

Deep neural networks have achieved impressive experimental results in image classification, but can surprisingly be unstable with respect to adversarial perturbations, that is, minimal changes to the input image that cause the network to misclassify it. With potential applications including perception modules and end-to-end controllers for self-driving cars, this raises concerns about their safety. This lecture will describe progress with developing automated verification and testing techniques for deep neural networks to ensure safety and security of their classification decisions with respect to input manipulations. The techniques exploit Lipschitz continuity of the networks and aim to approximate, for a given set of inputs, the reachable set of network outputs in terms of lower and upper bounds, in anytime manner, with provable guarantees. We develop novel algorithms based on feature-guided search, games and global optimisation, and evaluate them on state-of-the-art networks. We also develop foundations for probabilistic safety verification for Gaussian processes, with application to neural networks.

Marta Kwiatkowska is Professor of Computing Systems and Fellow of Trinity College, University of Oxford. She is known for fundamental contributions to the theory and practice of model checking for probabilistic systems. She led the development of the PRISM model checker, the leading software tool in the area. Probabilistic model checking has been adopted in diverse fields, including distributed computing, wireless networks, security, robotics, healthcare, systems biology, DNA computing and nanotechnology, with genuine flaws found and corrected in real-world protocols. Kwiatkowska was awarded two ERC Advanced Grants, VERIWARE and FUN2MODEL, and is a coinvestigator of the EPSRC Programme Grant on Mobile Autonomy. She was honoured with the Royal Society Milner Award in 2018 and the Lovelace Medal in 2019, and is a Fellow of the Royal Society, ACM and BCS, and Member of Academia Europea.

10:30-10:45 **Peter Davies**, (Thales)

What might I achieve with Verified Software in complex automotive systems

In the context of the Cyber Resilience methodology being developed by the Automotive Industry and the outcomes this must achieve, this talk will discuss the nature of a cyber-attack and the requirement for resilience. In the context of verified and verifiable software, we will address its potential role, effectiveness of as a means of countering cyber-attacks, and the contribution to the economics and some of the tools that may be required.

Peter is the Director Security Concepts at Thales. As a Technical Director of Thales in the UK Peter has been their leading expert on Cryptography in the UK responsible for providing cryptography and information security direction and expertise on a variety of products and projects. Previous work includes the development and certification of flexible and interoperable commercial security solutions that are also widely used by governments; these solutions are available worldwide and support the security of both communications and infomatics in an international, multi grade environment. Peter currently leads the Security Workstream for the Automotive Electronic Systems Innovation Network (AESIN) and security lead to the Innovate UK funded research programmes AutoDrive and RoboPilot. Peter is a frequent speaker at conferences and contributor to journals concerned with Automotive Cyber Security, CNI, Law Enforcement and Commercial security. Interested in the paradigm shift in security models that must accompany a more connected and less controlled environment.

10:45-11:15 Tea and Coffee break

11:15-12:00 **Joost-Pieter Katoen,** (RWTH Aachen University, Germany)
Separation Logic Goes Random

We marry two seminal deductive program verification techniques: weakest pre-expectations (WPEs) and separation logic (SL). WPEs are a quantitative analogue of Dijkstra's weakest pre-conditions used to reason about probabilistic effects such as coin flipping. SL enables logical reasoning about pointer programs and can deal with aliasing, memory leaks, null pointer dereferencing etc. We show that WPEs and SL can be combined in a natural and elegant way. The resulting quantitative separation logic (QSL) employs real-valued quantities instead of Boolean predicates and lifts the key SL connectives, separating conjunction and separating implication, from predicates to quantities. We will argue that QSL conservatively extends both WPEs and SL. QSL's wp-calculus is shown to be sound w.r.t. a simple operational semantics based on Markov decision processes, and preserves the frame rule, the key principle in SL enabling local reasoning about heaps. QSL enables reasoning about quantities such as the probability of terminating with an empty heap, the expected length of a list returned by a lossy list reversal algorithm, or the expected length of a path from the root to a leaf in randomised meldable heaps. QSL thus enables to reason about probabilistic programs mutating dynamic data structures in a compositional way purely at the source-code level.

Joost-Pieter Katoen is a Distinguished Professor with RWTH Aachen University, Germany, and is part-time professor at the University of Twente, The Netherlands. He received an honorary doctorate degree from Aalborg University, Denmark and holds an ERC Advanced Grant. His research interests include formal methods, model checking, concurrency theory, and probabilistic computation. He coauthored more than 75 journal papers and the book "Principles of Model Checking". He chaired the steering committee of ETAPS (2014-2019), is steering committee member of CONCUR, QEST, and FORMATS, and elected member of the Academia Europaea.

12:00-12:45 **Gustavo Petri** (Arm Ltd.)

Verification at Arm: a few case studies

The Security group within Arm Research is, in part, tasked with helping develop new technologies and capabilities to secure Arm technology and the wider Arm ecosystem. Formal verification techniques play an important role in helping us deliver on this, and as Arm's business and the wider semiconductor market evolves the Security group has a key role in delivering new analyses of the Arm architecture, as well as new verification capabilities. In this talk I will present (in various levels of detail) three different verification projects carried out by members of the Security group that have either recently completed, or are still underway, and until now have not been discussed outside of the company. One project, in particular, saw members of the Security group embedded alongside frontline product-group engineers to develop a verification methodology for low level security critical firmware for an unannounced product. This methodology, built around CBMC, was successfully delivered and is now in active use by the product group in question, integrated into the team's Continuous Integration flow: a successful adoption of software verification techniques by a production team.

Gustavo Petri is a Staff Research Engineer in the Security Research group. His research focuses in security, distributed systems, concurrency theory, formal methods, programming languages, and formal semantics. Before joining Arm Research, Gustavo was an Assistant Professor at the Université Paris Diderot — Paris 7, in the IRIF laboratory, and has also held positions at DePaul University in Chicago, and Purdue University in Indiana. Gustavo obtained his PhD in Computer Sciences from the Université de Nice — Sophia Antipolis in 2010.

12:45-13.45 Lunch and Poster session

Afternoon of Wednesday, 25th September 2019

13:45-14:30 **Sandrine Blazy,** (Inria Rennes, France)

Formal Verification of a Constant-Time Preserving C Compiler

Timing side-channels are arguably one of the main sources of vulnerabilities in cryptographic implementations. One effective mitigation against timing side-channels is to write programs that do not perform secret-dependent branches and memory accesses. This mitigation, known as «cryptographic constant-time», is adopted by several popular cryptographic libraries. This talk will focus on compilation of cryptographic constant-time programs, and more specifically on the following question: is the code generated by a realistic compiler for a constant-time source program itself provably constant-time? Surprisingly, we answer the question positively for a mildly modified version of the CompCert compiler, a formally verified and moderately optimising compiler for C. Concretely, we modify the CompCert compiler to eliminate sources of potential leakage. Then, we instrument the operational semantics of CompCert intermediate languages so as to be able to capture cryptographic constant-time. Finally, we prove that the modified CompCert compiler preserves constant-time. Our mechanisation maximises reuse of the CompCert correctness proof, through the use of new proof techniques for proving preservation of constant-time. These techniques achieve complementary trade-offs between generality and tractability of proof effort and are of independent interest.

Sandrine is Professor at the University of Rennes 1 and member of the Celtique team at IRISA - Inria Rennes. Her research interests include semantics, theorem proving, static analysis, compilation and software security. She made several contributions to the CompCert formally verified C compiler, and to the Verasco formally verified static analyser.

14:30-14:45 **Scott Owens**, (University of Kent / VeTSS)

Building Trustworthy Software with CakeML

CakeML is an impure functional programming language aimed at supporting formally verified programs. The CakeML project has several aspects including formal semantics and metatheory, a verified compiler, a mechanised connection between its semantics and higher-order logic (in the HOL4 interactive theorem prover), and an example verified theorem prover written in CakeML and HOL4. It also has respectable performance compared to industrial-strength implementations of ML. The CakeML project has been running for six years and has achieved its initial goal of demonstrating the feasibility of a practical, mechanically verified compiler from program source text to target machine code. But where should we go from here? In this talk, I will present an overview of the compiler, and the techniques we used to verify it. I will also give a high-level overview of the variety of ongoing projects in the CakeML ecosystem.

Scott Owens is a Reader at the University of Kent. Prior to that, he was a post-doc at Cambridge and did his PhD at the University of Utah. Besides the CakeML project, he has worked, among other things, on the semantics of weak memory concurrency for hardware (x86, and POWER) and software (C++11), specification languages for formal semantics (Ott and Lem), and ML-style module systems.

14:45-15:00 **Conrad Watt**, (University of Cambridge)

WebAssembly: Mechanisation, Security, and Concurrency

WebAssembly is the first new language to be introduced to the Web ecosystem in over twenty years. Its official specification is given as a formal semantics, making the language a perfect target for further applications of formal methods. This talk highlights recent work which builds on this formal semantics and discusses the ongoing development of WebAssembly's relaxed memory model, which is complicated by the language's inter-operation with JavaScript.

Conrad Watt is a PhD student at the University of Cambridge, supervised by Peter Sewell. His work focusses on the WebAssembly language, and he serves as an Invited Expert to the WebAssembly Working Group, assisting with the development of the language's relaxed memory model. He holds a Google Doctoral Fellowship in Programming Technology and Software Engineering.

15:00-15:15 **Brijesh Dongol**, (University of Surrey / VeTSS)

Mechanised Owicki-Gries Proofs for C11

The states of a program executing under a weak memory model (such as the C11 model) are typically formalised by a graph together with a set of axioms that describe validity. For a subclass of C11 (that disallows load-buffering cycles), prior work has shown how valid C11 states can be generated in an operational manner. This has paved the way for the development of high-level assertions over weak memory states, which has in turn enabled Owicki-Gries style reasoning of (restricted) C11 programs. We describe recent efforts in this direction, including an assertion language for C11, its integration into the Isabelle theorem prover, and its application to prove non-trivial examples. Interestingly, the Owicki-Gries proof methodology remains unchanged from the classical sequentially consistent setting.

Brijesh achieved a BSc in Computer Science and Mathematics and a BSc (Hons) in Logic and Computation, both from Victoria University of Wellington, New Zealand. In 2009, he completed a PhD on formal derivations of concurrent algorithms at the University of Queensland, Australia. After this, he held post doctorate positions at The University of Queensland and then at the University of Sheffield. He joined Brunel University London as a Lecturer in 2014 and moved to the University of Surrey as a Senior Lecturer in 2018. He is mainly interested in formal techniques and verification methods for concurrent and real-time systems. This includes concurrent abstractions, transactional memory and associated correctness conditions, weak memory models, and program algebras.

15:15-16:00 **Jeremy B,** (National Cyber Security Centre, UK)

Verification for High Assurance Systems

Within the National Cyber Security Centre (NCSC), we have explored the application of various tools and techniques from software and protocol verification to systems that require high levels of assurance, or that are designed to operate in high threat environments. I will discuss our approach to real-world whole system assurance, and describe the role of verification for us historically, now, and in the future, including some outline case studies. I will also set out some of our open questions for the research community – that is, areas where we believe that verification techniques can support our assurance role in the future, but where there are either currently gaps in knowledge, or gaps in practically usable techniques, and describe how we want to continue to work with the community to address them.

Jeremy is the Head of High Assurance Engineering Research at the National Cyber Security Centre (NCSC). The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. NCSC was launched in October 2016, bringing together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure.

16:00-16:30 Tea and Coffee break, end of Workshop

The Research Institute on Verified Trustworthy Software Systems (VeTSS) at Imperial is a UK Academic Research Institute in Cyber Security, funded by the Engineering and Physical Sciences Research Council.

EPSRC
Engineering and Physical Sciences
Research Council

National Cyber
Security Centre

Imperial College
London