RESEARCH INSTITUTE IN
VERIFIED TRUSTWORTHY SOFTWARE SYSTEMS

First VeTSS PhD School and Sixth Workshop on Formal Methods and Tools for Security (FMATS)

24-25 September, Microsoft Research, Cambridge

Speakers and talks

Monday, 24th September 2018

Karthikeyan Bhargavan,
Inria Paris -ERC Consolidator Grant

Verified Cryptography for Verified Protocols.

Karthikeyan Bhargavan (Karthik) is a directeur de recherche at Inria in Paris, where he leads a team of researchers working on developing new techniques for programming securely with cryptography. He was born in India and did his undergraduate studies at the Indian Institute of Technology Delhi and his PhD at the University of Pennsylvania. He then worked for several years at Microsoft Research in Cambridge before moving to France. Karthik's research lies at the intersection of programming language design, formal verification, and cryptographic protocol analysis. In the context of TLS, he co-discovered several attacks on TLS 1.2: Triple Handshake, FREAK, SMACK, LOGJAM, SLOTH, SWEET32. He is a member of the miTLS team that has built the first verified TLS implementations. He is currently working on Messaging Layer Security and on HACL, a verified library of modern cryptographic primitives.*

Suresh Jagannathan,
Purdue University and DARPA, USA

Learning for Automated Synthesis and Verification

Suresh Jagannathan is the Samuel D. Conte Professor of Computer Science at Purdue University. His research interests are in programming languages generally, with a specific focus on program verification, verified compilation, functional programming, and concurrent and distributed systems. From 2013 - 2016, he served as a program manager in the Information Innovation Office at DARPA, where he conceived and led programs in probabilistic reasoning and machine learning, software systems verification, and adaptive computing. He has also been a visiting faculty at Cambridge University, where he spent a sabbatical year in 2010; and, prior to joining Purdue, was a senior research scientist at the NEC Research Institute in Princeton, N.J. He received his Ph.D from MIT.

Mike Dodds,
Galois, USA

Continuous Verification in Industry

Mike Dodds is a Principal Scientist at Galois. He was previously a lecturer at the University of York. His research has covered a broad range of topics related to logic and verification. He has designed new logics aimed at concurrency verification as well as automated checking tools, semantic models for concurrency, and high-performance concurrent algorithms. Mike earned his PhD in Computer Science, and his masters degree in Software Engineering from the University of York. He is an Industry Fellow of the Royal Society, reflecting joint work with Microsoft Research.

Roderick Chapman,
Protean Code Ltd., UK

Murphy vs Satan: Why Programming Secure Systems is Still so Hard…

Rod is an independent consultant software engineer. He specializes in the development of safety and security-critical systems, from requirements engineering, through architectural design and implementation, to verification, audit and assessment. Following graduation, Rod joined Praxis (now Altran UK), and contributed to many of the company's keynote projects, rising to the role of principal engineer for software process and design. He also led the programming language and verification research group at Praxis, leading the technical development, training, sales and marketing of the SPARK product line. More recently, Rod turned his attention to software process, working on merging the discipline of traditional high- integrity processes with more agile approaches such as Scrum, and the philosophy of the Lean Engineering Movement. In February 2015, Rod was appointed Honorary Visiting Professor in the Department of Computer Science at the University of York.

Nadia Alshahwan,
Facebook

Sapienz: Automated Test Design and Bug Fixing

Nadia Alshahwan is a Software Engineer at Facebook. She is part of the Sapienz team and her main interests are improving the search based algorithm and optimizing the testing process. Nadia received a PhD from UCL in software testing. She also has a background in cyber security and finance. Her talk describes the deployment of Sapienz, a system for automated test case design that uses Search Based Software Engineering (SBSE) that has been deployed at Facebook since October 2017 to design test cases, localise and triage crashes to developers and monitor their fixes. It also describes SapFix, a system for automated fix design and deployment. Facebook continues to build on the Sapienz infrastructure, extending it to provide other software engineering services and the hope is that this will yield sustained interest in SBSE and hybridisation of it as a result. Finally, the talk also outlines some open problems and challenges for the SBSE community, based on their experience of deploying Sapienz at Facebook scale.

Antoine Delignat-Lavaud,
Microsoft Research Cambridge

Fully-Automated Verification of Low-Level Network Protocol Message Parsers

The code for parsing and formatting network messages is important both for security and for performance. For instance, some recent catastrophic bugs (such as Heartbleed, or a similar parser bug in CloudFlare's HTTP header processing in nginx) are caused by aggressive optimizations during parsing. Parsing malleability is another source of security vulnerabilities: for instance, an overflow in the ASN.1 processing of signatures in NSS led to a universal signature forgery attack. Over the past two years (and in collaboration with several interns), we have built a new set of tools to completely automate the generation and verification of parsing code from a C-like specification language used in IETF RFC (such as the one for TLS 1.3). Our toolchain consists of a verified library of parsing combinators, that can emit both high-level specifications (on pure, ML-like types) and low-level implementations (in Low, a fragment of F* that extracts to C). Our combinators prove the correctness of the parser specification (that is, that parsing is the partial inverse of serialization, and serialization is the inverse of parsing), and the safety of the low-level implementation. We also use an untrusted tool to translate RFC specifications into the appropriate calls to the combinator library. Using this toolchain, we are able to fully automate the verification of TLS 1.3 parsers in Everest. Antoine Delignat-Lavaud is a researcher at Microsoft. He is part of Project Everest, which aims to build and deploy a verified HTTPS stack.*

Kyndylan Nienhuis,
University of Cambridge

Formally Proven Security Properties of the CHERI-MIPS Research Architecture

CHERI-MIPS is an experimental instruction set architecture that adds hardware support for capabilities, letting one enforce fine-grain temporal memory safety and/or scalable software compartmentalisation.
CHERI guarantees that the permissions of available capabilities are monotonic until a domain boundary is crossed. The definition of this property was originally described in high-level prose, making it difficult to understand what it precisely says, let alone whether it is true. We formalised and proved this property, in Isabelle, and uncovered several bugs in CHERI-MIPS. Furthermore, we showed that our formalisation is strong enough to prove memory isolation in a specific example.
Kyndylan Nienhuis is a PhD student and Gates scholar at the University of Cambridge, working on the verification of basic security properties of CHERI.

Gernot Heiser,
Data61, Australia

Building secure systems with seL4

seL4 is arguably the most solid foundation for building safe and secure systems, thanks to its comprehensive formal verification, comprising functional correctness, isolation enforcement and worst-case execution-time analysis. In this talk I will discuss how these features can be used to build secure real-world systems and where present limitations are. I will outline some of our on-going activities for addressing some of these limitations, especially our work on providing time protection and the Cogent project, which aims to reduce the cost of ensuring the trustworthiness of critical user-level components.

Gernot Heiser is Scientia Professor and John Lions Chair of Operating Systems at UNSW Sydney and Chief Research Scientist at Data61, CSIRO. His research interest are in operating systems, real-time systems, security and safety. He is the founder and past leader of Data61's Trustworthy Systems group, which pioneered large-scale formal verification of systems code, specifically the design, implementation and formal verification of the seL4 microkernel; seL4 is now being designed into real-world security- and safety-critical systems. Heiser's former company Open Kernel Labs, acquired by General Dynamics in 2012, marketed the OKL4 microkernel, which shipped on billions of mobile wireless chips and more recently ships on the secure enclave processor of all iOS devices. Gernot is a Fellow of the ACM, the IEEE and the Academy of Technology and Engineering (ATSE).

Tuesday, 25th September 2018

Nikos Gorogiannis,
Facebook and
Middlesex University

RacerD: Finding Races in Java Code

Nikos works with the Facebook Infer team on static analysis, and as a Senior Lecturer in Computer Science at Middlesex University. He is interested in applied verification, logic and automated reasoning. He previously led the development of Cyclist, a theorem prover based on cyclic proof, and worked on several decision procedures and complexity results for separation logic.

Towards Fast Taint Analysis

Dynamic taint analysis is a fundamental technique for software security that has been used, amongst others, for vulnerability analysis and runtime attack detection. However, it is known to face scalability issues. In his talk, he discusses methods for efficient taint analysis to improve its practical use.

John Galea is reading for his DPhil at the University of Oxford under the supervison of Daniel Kroening. His main interests include binary analysis with the goal of discovering and assessing security vulnerabilities.

John Galea
Diffblue and University of Oxford

GraphicsFuzz: a Pseudo-Random Journey from Formal Verification to Android Graphics Testing

I recently joined the Android Graphics Team at Google after Google acquired GraphicsFuzz, a spin-out from Imperial that I founded with my former postdoc Hugues Evrard and former PhD student Paul Thomson. In the talk I will briefly outline the GraphicsFuzz journey, starting from work on formal verification of "general-purpose GPU" (GPGPU) software in 2011, getting interested in GPGPU compiler fuzzing in 2014, switching to non-GPGPU (i.e. just GPU) compiler fuzzing in 2015, going through entrepreneurship training in 2017, and spinning out and selling GraphicsFuzz in 2018. I'll also reflect a bit on the different challenges associated with having practical impact via verification vs. testing, the pros and cons of open source, and some of the pleasures and pains we experienced during the university spin-out process.

Alastair Donaldson is a Software Engineer at Google, and a Reader and EPSRC Early Career Fellow in the Department of Computing at Imperial College London. At Google he leads a group within the Android Graphics specialising in automated fuzzing of graphics drivers, building on research work he pioneered at Imperial and commercialized via the GraphicsFuzz spin-out company, which Google acquired in 2018. At Imperial he leads the Multicore Programming Group, investigating novel techniques and tool support for programming, testing and reasoning about highly parallel systems. He was the recipient of the 2017 BCS Roger Needham Award, has published 80+ articles on programming languages, formal verification, software testing and parallel programming, and coordinated the FP7 project CARP: Correct and Efficient Accelerator Programming. Alastair was previously a Visiting Researcher at Microsoft Research Redmond, an EPSRC Postdoctoral Research Fellow at the University of Oxford and a Research Engineer at Codeplay Software Ltd. He holds a PhD from the University of Glasgow, and is a Fellow of the British Computer Society.

Alastair Donaldson,
Google, UK

Anindya Banerjee,
NSF, USA

Relational Contracts and Logics

Anindya Banerjee is a Program Director in the Computing and Communications Foundations Division of the Directorate for Computer & Information Sciences & Engineering at the US National Science Foundation. In this role he is associated with the Formal Methods in the Field program, the Scalable Parallelism in the Extreme program, and the Software and Hardware Foundations program. His research interests are in the principles of programming. Anindya is also an affiliate faculty at the IMDEA Software Institute, Madrid, where, until 2016, he was full professor. Prior to that he was full professor of Computing and Information Sciences at Kansas State University, USA. He was a recipient of the Career Award of the National Science Foundation in 2001.

Sofia Guerra,
Adelard, UK

Assuring safety-critical COTS components for the nuclear industry

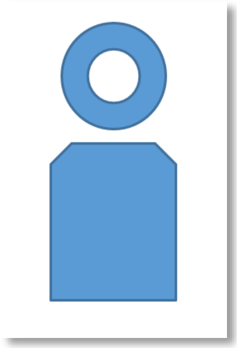
Sofia Guerra is a partner at Adelard and she leads Adelard work on the nuclear sector. Since joining Adelard in 2000, she has led numerous projects funded by the UK, French, Finnish, US and Swedish nuclear industry, regarding the safety assessment, justification and reliability estimation of a variety of software-based systems, including the assessment of smart devices software, PLC-based systems as well as FPGA-based systems. She has been involved in writing standards and regulations for licensees, and she leads a number of research projects funded by the nuclear industry internationally. In addition to the nuclear industry work, Sofia was part of the Independent Safety Advisor/Auditor team for several UK defence projects. She was registered as a software expert with the Medicines and Healthcare products Regulatory Agency in the UK and has assessed the software component of several medical devices. Sofia Guerra is a Chartered Engineer. She has a degree in Mathematics and Computer Science (1989–1994) and a PhD in Mathematics (1999), both from Lisbon Institute of Technology, Portugal, and a BMus (1990). Prior to joining Adelard, she was a Research Fellow in the Department of Computer Science, University College London, where she was working on Requirements Engineering.

Verified Hardware Compilation

John Wickerson is a Research Fellow in the Department of Electrical and Electronic Engineering at Imperial College London. His research focuses on high-performance computing with the help of formal methods with the aim of improving reliability. His latest project investigates the interaction between transactions and weak memory and he has previously worked on compiling weakly-consistent concurrent software into hardware, on *generating test-cases for memory consistency models, on formalising the concurrency semantics of C/C++ and OpenCL, on diagrammatic proofs about programs, and on software verification using the rely/guarantee method.*

John Wickerson,
Imperial College
London and VeTSS

Effpi: Concurrent Programming with Dependent Behavioural Types



Alceste Scalas is a Research Associate at Imperial College London, Dept. of Computing. Before his PhD, he worked as software developer in industry, and as research software engineer at CRS4 (Centre for Advanced Studies, Research and Development in Sardinia). He is interested in the theory and practice of concurrent and distributed systems: how to design and develop correct and reliable applications, by building upon rigorous mathematical foundations. His main research topics include concurrency theory, distributed systems, programming languages, and type systems; he is particularly keen on producing theoretically-grounded software tools and libraries to aid software design, development, and verification.

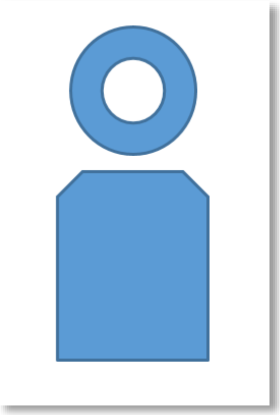
Alceste Scalas
Imperial College
London and VeTSS

Automated black-box verification via model learning

Matteo Sammartino is Research Associate and Teaching Fellow at University College of London. His research is focussed on Categorical models of formal languages, Algebraic and coalgebraic specification, Process calculi and Petri nets and Automata learning.

Matteo Sammartino,
University College
London and VeTSS.

Sail and theorem-prover ISA Semantics for ARMv8-A, RISC-V, and CHERI-MIPS



Thomas Bauereiss is research associate in the group of Prof Peter Sewell, working in the REMS: Rigorous Engineering for Mainstream Systems project on the formal modelling and verification of Instruction Set Architectures. Previously, he worked on techniques for verifying information flow security at DFKI Bremen in the DFG priority programme Reliably Secure Software Systems (RS3).

Alasdair Armstrong and **Thomas Bauereiss**, University of Cambridge

Alasdair Armstrong is research assistant at Cambridge University working with Prof Peter Sewell on the REMS project. Alasdair completed his PhD at the University of Sheffield under the supervision of Dr. Georg Struth, working on algebraic formal methods and rely-guarantee. His current research interests primarily lie in using formal methods to verify real-world programs, especially concurrent programs, and the use of interactive and automated theorem proving technology in this area. He is also interested transactional memory and dependently-typed functional programming.