



UK RESEARCH INSTITUTE ON

**VERIFIED
TRUSTWORTHY
SOFTWARE
SYSTEMS**

ANNUAL REPORT 23/24

CONTENTS

Foreword (NCSC representative)	3
Directors' Message	4
Overview of 2023/24	5
VeTSS Problem Book 2024	7
VeTSS Website	8
VeTSS Events	9
VeTSS Problem Definition Workshop (January 2024)	9
VeTSS Advisory Board Meeting (February 2024)	10
Annual Conference (May 2024)	10
VeTSS Summer School (August 2024)	12
Formal Specification and Validation at Scale (October 2024)	14
Sponsored Events	15
Women in Logic 2024 (July 2024)	15
Kent Concurrency Workshop and S-REPLS 15 (July 2024)	16
VeTSS-Aligned Projects (2023/24)	17
Making Memory Management More Secure (M4Secure)	18
SecuriTy SummaRies for SecUre SofTwarE Development (TRUSTED)	19
Safe And seCure REmote Direct Memory Access (SACRED-MA)	20
VeTSS Publications 2024	21
Equality, Diversity and Inclusion	22



FOREWORD

(NCSC REPRESENTATIVE)

VeTSS has gone from strength to strength this year. VeTSS has always been intent on strengthening and supporting the verification community, and this year is no exception. They have been involved in a range of events aimed at all levels of the community on a plethora of topics. We have seen the annual VeTSS Summer School establish itself as a pillar in the early career verification researcher calendar, providing an insight into the breadth of work going on, world-class speakers on cutting-edge topics and growing a sense of camaraderie and forging important contacts and relationships. The typically outstanding VeTSS annual event also excelled at showcasing the work going on in the VeTSS community at a national scale, as well as providing a joint forum for academia and industry to communicate, with leaders from both worlds participating heavily.

We've also seen the landmark four-week Big Specification event take place at the Isaac Newton Institute in Cambridge this autumn. This large-scale programme provided the opportunity for researchers and verification professionals from all over the world to get together and collaborate over an extended period. We saw significant involvement from the VeTSS directors and community in both organising and participating in this event, with several targeted workshops taking place throughout.

Notable in its scale, ambition and global participation was the two-day Formal Specification and Validation at Scale event, aimed at increasing the uptake of Formal Methods. This had involvement not only from leading researchers in academia and some of the most influential people in industrial formal methods, but also government, hosting talks from the White House, NCSC, DARPA and NSA.

However, community building is only part of VeTSS remit. This year VeTSS has extended its history of funding and supporting important, impactful research in the field of verified trustworthy software systems. VeTSS continues to provide guidance and leadership in this field and this year we've seen the publication of the VeTSS Problem Book, aiming to clarify the most important verification problems and challenges facing the community today. We have already observed the impact this has had and anticipate its continuing effect going forward.

This has been a strong year for VeTSS and NCSC anticipates the work done this year, setting the research institute up for prolonged success in the future.

Adam W1, NCSC

DIRECTORS' MESSAGE

We are delighted to have led VeTSS through another successful year, realising its core vision of by the community, for the community. This has been a year of growth, consolidation and transformation, thanks to recent breakthroughs and advancements in AI, quantum and hardware technologies. These have posed new verification challenges and opportunities, further highlighting the importance of the research by the VeTSS community in providing trustworthy systems underpinned by rigorous mathematical proofs.

Thanks to the tireless efforts of our dedicated Advisory Board and members of the VeTSS community, we have compiled the first VeTSS Problem Book, a repository of key verification problems and challenges important to the VeTSS community, including academia, industry and the government. The VeTSS Problem Book is an important part of our community-building strategy, focusing the verification landscape on the problems that the VeTSS community should tackle, shaping the growth of verification research nationally.

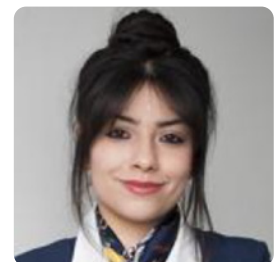
We have seen continued progress on the VeTSS-aligned projects, with all three producing strong publications in some of the top venues in the field. These have ranged from formal models of real hardware (which corrected inaccuracies in informal technical specifications) and automated static analysis of security flaws to theoretical and practical advances in model checking large-scale systems.

This has been coupled with strong community engagement and facilitation of training, mentorship and networking opportunities through our Annual Meeting, VeTSS Summer School and support of workshops and meetings such as the Concurrency Workshop and South of England Regional Programming Language Seminar (S-REPLS). We also played a significant role in the four-week Big Specification event held at the Isaac Newton Institute, with an internationally significant two-day Formal Specification and Validation at Scale event, which was attended by speakers from the White House, DARPA, NCSC, AWS, Microsoft, Meta and many other industrial and academic stakeholders. We are proud to have facilitated engagement between academia, industry and government, and provided pathways to interdisciplinary collaboration.

Our vision in our third year as directors is to lead VeTSS along this growth trajectory, supporting verification research and enhancing its impact, while acknowledging the evolving landscape of computing and recognising the UK's diversity and expertise in verification.



Brijesh Dongol



Azalea Raad

OVERVIEW OF 2023/24

VeTSS, a Research Institute funded by the National Cyber Security Centre (NCSC), is bringing together academia, industry, regulators and government stakeholders to tackle critical software security and safety challenges in the UK.

This year has brought transformative progress, innovative partnerships, and a strong commitment to building truly dependable software systems. Looking ahead, we will continue to hold regular events for the community and will pursue groundbreaking initiatives to redefine digital reliability and drive innovation across diverse industries.

PROBLEM BOOK 2024

We launched the inaugural VeTSS Problem Book 2024, a comprehensive document outlining essential research topics and challenges crucial to the UK's strategic cybersecurity landscape. This publication was developed in close collaboration with our Advisory Board and an independent Expert Review Committee.

EVENTS

Our 2024 calendar was marked by significant events that fostered knowledge exchange and collaboration:

VeTSS ANNUAL CONFERENCE

A vital platform for interdisciplinary dialogue, connecting experts across quantum computing, artificial intelligence, and software verification. The conference successfully identified key research challenges and explored potential collaborative opportunities.

VeTSS SUMMER SCHOOL

Hosted at the University of Bristol in August, this event provided invaluable training and networking opportunities for emerging researchers and students in the field of software systems security.

FORMAL SPECIFICATION AND VALIDATION AT SCALE WORKSHOP

Hosted at the Isaac Newton Institute, Cambridge, it aimed to provide a meeting ground to facilitate interactions and exchanges between representatives of academia, research and industry, relevant to the theme, with the objective of identifying points of mutual interest and possible co-activity.

VeTSS SUPPORTED TWO NOTABLE WORKSHOPS:

- ‘Women in Logic 2024’ in Tallinn, Estonia (July 9)
- ‘Kent Concurrency Workshop and S-REPLS 15’ (July 18-19)

VeTSS-ALIGNED RESEARCH PROJECTS

Three strategic projects exemplify our commitment to advancing software system security:

TRUSTED. Focuses on establishing provable security for modern software that incorporates third-party code.

M4Secure. Developing an open-source framework for customisable memory management libraries.

SACRED-MA. Advancing understanding of Remote Direct Memory Access (RDMA) through rigorous verification methodologies.


FUNDING AND PARTNERSHIPS

We secured \$10,000 in sponsorship from AWS for the Formal Specification and Validation at Scale workshop. While a recent Network Plus proposal was not successful, we remain dedicated to exploring funding opportunities.

VeTSS PROBLEM BOOK 2024

Following a few rounds of revision, the VeTSS Problem Book was published in June 2024. The aim of the VeTSS Problem Book is to present VeTSS problems to the general community (academia, industry and government) and explain why these problems are important and why they motivate people.

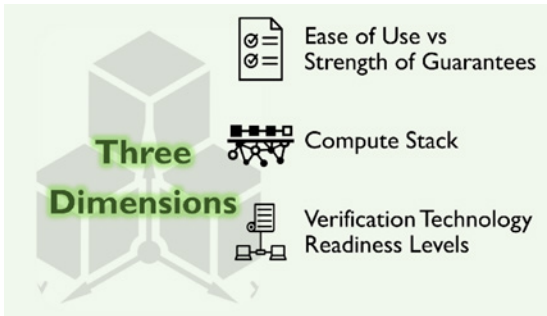
Our aim is to help researchers understand, improve, and deliver the impact of their existing work, and connect with others working on adjacent topics. The focus is not on what has been achieved, but on describing what we want to achieve, and how we would like to grow the field of verification. This will allow us to develop a research community that focuses on specific problems or can be encouraged to focus on them.




The VeTSS Problem Book is available online at tinyurl.com/VeTSS-ProblemBook2024 and through the QR code.

We have identified a need to explore verification technologies across three different dimensions: lightweight vs heavyweight techniques (where we balance the ease of use against the strength of the guarantees), the compute stack, and the readiness level of a particular verification technology.


These dimensions cover six key verification themes: specification, resilience, protocols, software, programmer support and proof/program robustness. By presenting these challenges and opportunities, we aim to stimulate innovation and collaboration within the verification research community.





IMPACT

The Problem Book was a key tool that helped lead a discussion session on *'Bringing together academia, government and industry'* at the Formal Specification and Validation at Scale Workshop at the Isaac Newton Institute.







INI Seminar Room 1




The VeTSS Problem Book
(and discussion on working together)

Brijesh Dongol
UNIVERSITY OF SURREY

Azalea Raad
Imperial College London

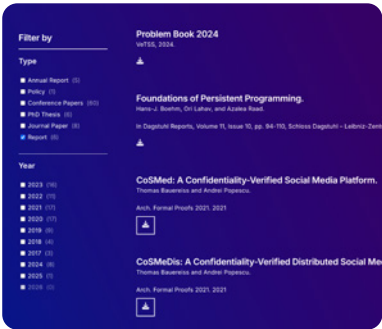


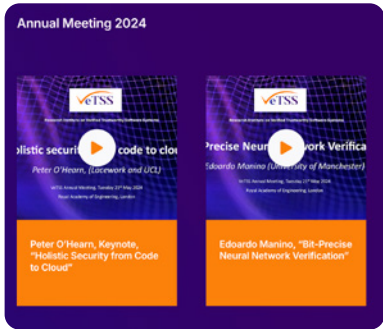






The new VeTSS website was launched in October 2024. This updated version introduced several new features to enhance user experience and accessibility:



A searchable index of all publications and news articles



An archive section housing videos of recordings from past events



A blog to host the short articles from the VeTSS community

These improvements have been made with the aim to make the website a more valuable resource for the verification and trustworthy systems community.



VETSS.ORG.UK

VeTSS EVENTS

VeTSS PROBLEM DEFINITION WORKSHOP

JANUARY 2024, BCS LONDON

The VeTSS Problem Definition Workshop took place on January 12, 2024, at the BCS London, building on discussions from the 2023 Advisory Board meeting. It aimed to refine the VeTSS Problem Book, which focuses on key verification challenges for system robustness, maintainability, and assurance. Chaired by Prof. Chris Hankin, the workshop featured an overview of the Problem Book's themes, followed by two sessions: one for feedback on the draft and another for in-depth discussions on verification topics to shape the next iteration.

The other contributors to the problem definition workshop were Rob Ashmore and Matthew Hill (DSTL), John Wickerson (Imperial College London), Steve Schneider (University of Surrey), Martin D2 and Adam W1 (NCSC) and Ana Cavalcanti (University of York). Thank you to everyone who participated, and special thanks to Chris Hankin for his expert guidance as chair. This collaborative effort was a testament to the dedication of our community in advancing the field of verification.



Chris Hankin
Imperial College London



John Wickerson
Imperial College London



Steve Schneider
University of Surrey



Ana Cavalcanti
University of York

VeTSS ADVISORY BOARD MEETING

FEBRUARY 2024,
IMPERIAL COLLEGE LONDON

The VeTSS Advisory Board meeting reviewed VeTSS' achievements, ongoing projects, and upcoming initiatives, including a website redesign. Key discussions focused on refining the Problem Book, evaluating Verification Technology levels, and exploring collaborations with other Research Institutes, particularly a joint Network Plus grant application. Advisory Board members provided critical feedback on six key themes of the Problem Book, guiding its next iteration before the VeTSS Annual Conference in May 2024. The meeting concluded with discussions on new funding opportunities, reinforcing VeTSS' commitment to advancing verification research through collaboration and strategic planning.

ANNUAL CONFERENCE

MAY 2024,
ROYAL ACADEMY OF ENGINEERING, LONDON

The VeTSS Annual Conference 2024 brought together leading researchers in verification, testing, and program analysis. The event featured a series of talks and panel discussions aimed at:

- Showcasing state-of-the-art research
- Identifying open challenges
- Exploring cross-pollination opportunities across VeTSS themes.

The VeTSS Annual Conference 2024 reinforced VeTSS' role as a central hub for collaboration and innovation in verification research. The insightful talks and discussions showcased the breadth and depth of ongoing work in the field. The VeTSS organising team would like to thank all the speakers for their valuable contributions to the conference.



Prof. Peter O'Hearn
(Lacework and UCL)
youtu.be/ttUxPPGRcd8

OPENING AND KEYNOTE

The conference kicked off with a welcome and introductions from the VeTSS directors. They highlighted achievements over the past year. Peter O'Hearn (Lacework and UCL) then delivered the keynote talk, '*Holistic Security from Code to Cloud*', addressing the importance of securing the entire software stack.

MORNING SESSION



Bit-Precise Neural Network Verification
Edoardo Manino,
University of Manchester
youtu.be/5h_utb3_EBI



Object Capabilities as Guards – Specification, Verification, and Open Calls
Sophia Drossopoulou,
Imperial College London
youtu.be/ONRQuPhVHFY



Contactless Payments Made Private via Bisimilarity
Ross Horne,
University of Strathclyde
youtu.be/XVqBKy-larE

AFTERNOON SESSION

Industry perspectives



Writing Formal Specifications at ARM
Jade Alglave, ARM
youtu.be/Q2GiW9263lo



RISC-V Processor Verification: Challenges and Opportunities for Formal
Ashish Darbari, Axiomise
youtu.be/5sDQA89-OGk



Verification and Legal Consequences
Peter Davies, Thales
youtu.be/Lye6OFx4Llk

VeTSS-aligned projects



SACRED-MA
Gregory Chockler, University of Surrey
Guillaume Ambal,
Imperial College London
youtu.be/vD8YG3qDqoU



TRUSTED
Narges Khakpour,
Newcastle University



M4Secure
Zheng Wang,
University of Leeds
youtu.be/5Mvd8rfr-7E

Short talks



Using Program Synthesis to Make Your Code Run Faster
Elizabeth Polgreen,
University of Edinburgh
youtu.be/6X26G6qW7SI



Secure Smart Contracts with Isabelle/Solidity
Diego Marmoler,
University of Exeter
youtu.be/cwZblCN72J8

VeTSS SUMMER SCHOOL

AUGUST 2024, UNIVERSITY OF BRISTOL



A very successful VeTSS Summer School brought together students from across the UK this summer to attend specialist lectures in program analysis, testing, and verification. The three-day event, held at the University of Bristol, August 13-15, offered an enriching environment for knowledge exchange and collaboration.

Special thanks go to our expert lecturers and our colleagues at the University of Bristol who hosted us and whose support was invaluable to make the Summer School possible. We are very grateful to all participants, speakers and organisers, for their contributions and their commitment to help shape the future of verification, testing, and program analysis research.

PROGRAMME HIGHLIGHTS

The Summer School began with a welcoming pizza social evening at the Department of Computer Science, setting a friendly tone for the days ahead. The sessions included lightning talks by the participants, who shared their research interests, immediately creating connections and sparking collaborative discussions.



LEARNING ENVIRONMENT

The historic Fry Building provided an inspiring backdrop for our activities, with its sunny courtyard offering the perfect space for informal discussions during breaks. Six distinguished experts in the field led comprehensive lectures and interactive workshops, ensuring a rich learning experience that combined theoretical knowledge with practical applications.



THE SIX MAIN LECTURES ARE SHOWN BELOW



Fantastic Morphisms and Where to Find Them

Nicolas Wu,
Imperial College London
youtu.be/9l7LxtRRRiq



Synthesis & Verification of CHERI Memory Managers

Jeremy Singer,
University of Glasgow
youtu.be/4xa3jcRfqZq



A Pyramid Of (Formal) Software Verification

Martin Nyx Brain, City,
University of London
youtu.be/BIGZuQIESRU



Relaxed memory concurrency semantics and reasoning

Mark Batty, University of Kent
youtu.be/zKALBxsrU2o



Formal Verification of Privacy in Cryptographic Protocols: Theory and Practice

Ioana Boureanu,
University of Surrey
youtu.be/XGxeSpCWzro



Whole Systems Energy Transparency

Kerstin Eder,
University of Bristol
youtu.be/oDwsuAK5ifs

IMPACT AND ACKNOWLEDGMENTS

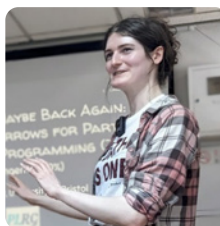
The Summer School succeeded in its mission to:

- Foster collaboration among emerging researchers,
- Provide hands-on experience with cutting-edge techniques,
- Create networking opportunities for future partnerships, and
- Inspire innovative approaches in program analysis and verification.

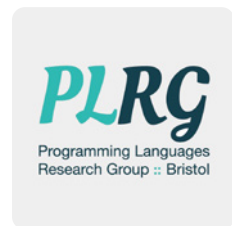
Special appreciation goes to our expert lecturers and the Programming Languages Research Group (PLRG) at the University of Bristol's Department of Computer Science for hosting this year's event and their indefatigable support. PLRG members Dr. Meng Wang and Jessica Foster arranged the historic Fry Building as our venue, with Jess also recording all the Summer School sessions. Their contributions have helped in shaping the future of verification, testing, and program analysis research in the UK.



Dr Meng Wang
University of Bristol



Jess Foster
University of Bristol



plrg-bristol.github.io

FORMAL SPECIFICATION AND VALIDATION AT SCALE

OCTOBER 2024, ISAAC NEWTON INSTITUTE, CAMBRIDGE

This Open for Business event was part of an INI programme on Big Specification. It was organised by the former VeTSS director (Philippa Gardner) and the current VeTSS directors. This workshop was supported by funding from VeTSS and Amazon Web Services.

Full details can be found here: gateway.newton.ac.uk/event/OFBW70

BACKGROUND

The computing industry still relies on informal methods such as prose specifications and ad hoc testing, leading to widespread errors and security vulnerabilities. These limitations have caused severe consequences, including cyberattacks and significant economic losses. To address this, there is a need for formal scientific and mathematical approaches to software specification, verification, and testing. Recent advancements, including proof assistants and analysis tools, show promise, but their integration into industry remains limited. A 2024 White House report emphasises the importance of formal methods and memory-safe programming to improve cybersecurity.

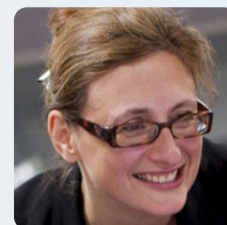
This event aimed to facilitate interactions and exchanges between representatives of academia, research and industry, relevant to the theme, with the objective of identifying points of mutual interest and possible co-activity. The focus was to examine the role of formal methods in industrial design, review the current and potential future capabilities of our tools and techniques, and discuss strategies for advancing their standardisation. The objective was to identify ways to progressively integrate formal methods into industrial

processes and to outline possible next steps, including how government support can facilitate this progression.

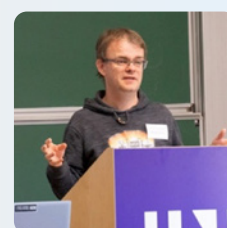
EVENT SUMMARY

The meeting featured talks by experts from academia, industry and government, including a talk on *'Back to the Building Blocks'* by Anjana Rajan from the Office of the White House and an afternoon session of talks from DARPA, NSA and NCSC. It brought together an audience of invited experts and policymakers from across academia, industry and government, all driven by a common goal to advance formal methods and strengthen cybersecurity. The event was recorded, with an edited version made available on YouTube.

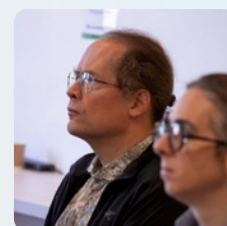
Several VeTSS Advisory Board members gave talks in the meeting, including Peter O'Hearn, Peter Sewell, Ekaterina Komendantskaya, Sophia Guerra, and Brad Martin. The VeTSS directors led a discussion session on *'Academia, Industry and Government Working Together to Use Formal Specifications at Scale'*. NCSC representative Paul W2 co-hosted a panel discussion. Adam W1 also gave a talk on *'Formal Methods for Cyber Security'*.



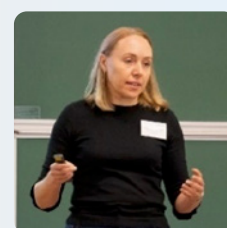
Philippa Gardner
Imperial College London



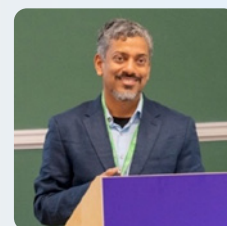
Matthew Parkinson
Microsoft (UK)



Peter Sewell
University of Cambridge



Ekaterina Komendantskaya
University of Southampton



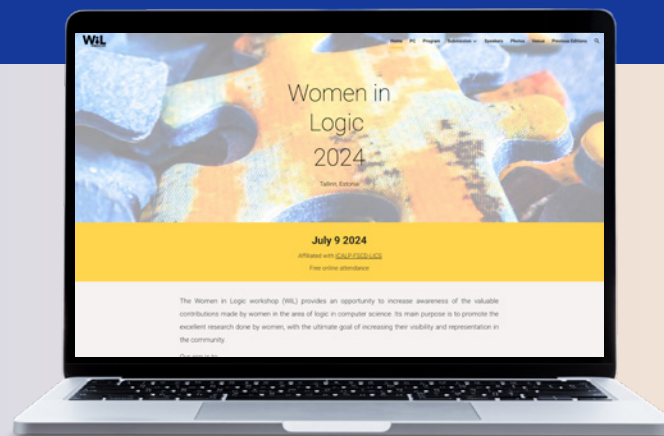
Swarat Chaudhuri
Google & University of Texas

Credit: Photos in this section by Isaac Newton Institute for Mathematical Sciences.

SPONSORED EVENTS

WOMEN IN LOGIC 2024

TALLINN, ESTONIA, JULY 9 2024



VeTSS was one of the sponsors of the Women in Logic Workshop (WiL), which provided an opportunity to increase awareness of the valuable contributions made by women in the area of logic in computer science. Its main purpose was to promote the excellent research done by women, with the goal of increasing their visibility and representation in the community. VeTSS Advisory Board member Greta Yorsh from Jane Street was one of the invited speakers.

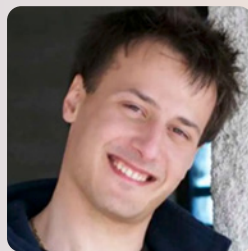
This event aimed to:

- Provide a platform for women researchers to share their work and achievements,
- Increase the feelings of community and belonging, especially among junior faculty members, post-docs and students, through positive interactions with peers and more established faculty members,
- Establish new connections and collaborations,
- Foster a welcoming culture of mutual support and growth within the logic research community.

KENT CONCURRENCY WORKSHOP AND S-REPLS 15

UNIVERSITY OF KENT, JULY 18-19, 2024

The South of England Regional Programming Languages Seminar (S-REPLS) and Concurrency Workshop took place on July 18-19, 2024, at the University of Kent, attracting 60+ attendees from academia and industry. Sponsored by VeTSS and the University of Kent, the event explored advances in programming languages and concurrency, featuring talks by Nicolas Wu (Imperial College London) on algebraic effects in functional programming, and Peter O'Hearn (UCL) on formal verification in industry.



Marco Paviotti, organiser
University of Kent

The Concurrency Workshop addressed challenges in multi-core and distributed systems, covering topics such as formal verification, functional programming, concurrency, type theory, and category theory. A special memorial talk by Simon Thompson honored David Turner, a pioneering figure in functional programming and creator of the Miranda language, which influenced Haskell.

The event fostered a collaborative and inclusive atmosphere, encouraging discussions and networking among researchers at all levels. The success of S-REPLS 15 and the Kent Concurrency Workshop highlights their importance in advancing programming languages and concurrency research.





VeTSS-ALIGNED PROJECTS (2023/24)

In 2022, the EPSRC, NCSC and the DSTL jointly agreed to fund a number of research projects aligned with the NCSC-funded Research Institutes ukri.org/opportunity/research-aligned-with-cybersecurity-research-institutes

Within this call, three VeTSS-aligned projects were funded, which together received £3.4M of investment. You will find the progress and impact they have achieved in the first two years of their research.



MAKING MEMORY MANAGEMENT MORE SECURE (M4SECURE)

OBJECTIVES

M4Secure is developing an automated framework for high-performance, secure memory allocators by leveraging hardware security features. It combines machine-learning-based code optimisation with formal verification to ensure security properties. The project focuses on AI-driven code synthesis and model checking to generate reliable dynamic memory management libraries with proven correctness and safety guarantees.



Jeremy Singer
University of Glasgow



Alice Miller
University of Glasgow



Zheng Wang
University of Leeds



PROGRESS

The project focuses on optimising application performance and enhancing memory security using automated and AI-driven techniques.

Key developments include:

- **Automated Super-Optimisation Framework:** Achieved a 5% performance boost in the llama.cpp application — a C++ implementation of the Meta Llama large language model — by applying instruction-level transformations without manual intervention.
- **Evaluation on SPEC CPU 2017:** Benchmarks ported to the Morello platform, assessing CHERI's memory security features in purecap and hybrid modes.
- **Open-Source Memory Allocators:** Porting and integrating widely used allocators into an optimisation workflow to study performance impacts.
- **Machine Learning for Memory Strategy Selection:** Developing an AI model to automatically choose the best memory allocator for specific applications.
- **Formal Verification:** Translating dynamic memory allocators into Promela and Dafny for correctness verification.
- **CHERI Memory Allocators & MicroPython:** Researching secure allocators and runtimes, particularly for MicroPython.

IMPACT

Key highlights of the study:

- **Memory Allocation on Secure Hardware:** Identified performance bottlenecks and optimisation opportunities on CHERI-enabled Morello platforms.
- **AI & Super-Optimisation for Memory Allocators:** Preliminary results show that machine learning enhances memory allocator design, emphasising the need for application-specific features in optimisation frameworks.
- **AI SuperConnector Award:** The project, which combines static code analysis and dynamic symbolic execution for bug detection, received a £20K seed fund for commercialisation. Collaboration with the University of Leeds commercialisation team is underway.
- **Open-Source Contributions:** Promela and Dafny code for simple allocators available at GitHub.
- **Research Lectures:** Delivered at three summer schools — SICSA (Aberdeen), Strathclyde (Glasgow), and VeTSS (Bristol) — covering cybersecurity and cybercrime topics.

SECURITY SUMMARIES FOR SECURE SOFTWARE DEVELOPMENT (TRUSTED)

OBJECTIVES

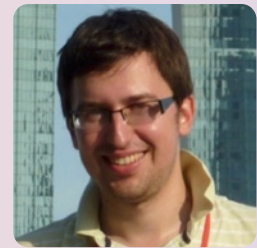
TRUSTED aims to enhance program security by designing efficient algorithms to generate and maintain security summaries for Java and Rust programs. It seeks to develop theories that refine and compose these summaries, improving precision and enabling cross-language information flow analysis. Additionally, it focuses on creating validation and lightweight verification techniques to assess the security of third-party libraries. Developers will receive meaningful feedback to help eliminate illegal information flow, ensuring more secure software. The effectiveness of these techniques will be evaluated through real-life case studies.



Narges Khakpour
University of Newcastle



Sven Schewe
University of Liverpool



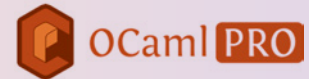
Dominik Wojtczak
University of Liverpool

PROGRESS

We have developed a technique and its supporting tool, Symmaries, to generate security summaries for Java applications, demonstrating scalability by analysing large codebases. Work has also begun on verifying the Google OAK restricted kernel in Rust, starting with memory isolation before extending to security summaries for Rust programs. Additionally, research is being conducted on formal threat analysis to address vulnerabilities, particularly in untrusted third-party libraries. Early studies are also exploring automated security analysis using automata-based techniques and reinforcement learning, though further work is needed to fully develop the anticipated security summaries.



We have started exploring the opportunities for commercialising Symmaries. Our initial market research shows interest from industry.



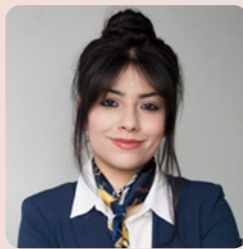
SAFE AND SECURE REMOTE DIRECT MEMORY ACCESS (SACRED-MA)

OBJECTIVES

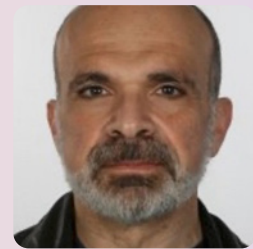
Remote Direct Memory Access (RDMA) is a modern technology enabling networked machines to exchange information without involving the operating system of either side, and thus significantly speeding up data transfer in computer clusters. This project aims to build up the understanding of RDMA from hardware models to distributed applications. We use formal approaches to develop and adapt reasoning techniques and proof methods to the unique design challenges of RDMA. Our goal is to develop tools to empower programmers and future developers of RDMA-based systems.



Brijesh Dongol
University of Surrey



Azalea Raad
Imperial College London



Gregory Chockler
University of Surrey

PROGRESS

Our main result is a formalisation of the core semantics of RDMA, with both an operational and a declarative semantics proved equivalent. Leveraging this formalisation, we have provided practical guidelines for writing efficient and reliable RDMA programs. Our current focus is on formalising RDMA libraries that provide shared data structures and network-wide synchronisation mechanisms. We have identified several bugs in existing implementations of these tools, highlighting the inherent complexity of RDMA semantics even for experienced developers. We are developing reasoning techniques to specify library behaviours, modularly combine independent libraries, and verify that implementations adhere to their intended specifications. We are also looking into using these libraries for efficient data replication. With this, we aim to demonstrate how traditional shared-memory properties can be achieved using RDMA data structures.

IMPACT

Our collaboration with NVIDIA engineers revealed that existing implementations do not fully leverage the weakness offered by the RDMA specification. We also discovered and reported several bugs in the 'Library of Channel Objects' (LOCO) library [Hodgkins & Izraelevitz]. These issues have been resolved by the developers, who provided updated versions of the impacted methods.





VeTSS PUBLICATIONS 2024

Guillaume Ambal, Brijesh Dongol, Haggai Eran, Vasileios Klimis, Ori Lahav, Azalea Raad. 2024. Semantics of Remote Direct Memory Access: Operational and Declarative Models of RDMA on TSO Architectures. In: Proceedings of the ACM on Programming Languages, Volume 8, Issue OOPSLA2. Article No.: 341, Pages 1982 – 2009. doi.org/10.1145/3689781

Narges Khakpour, Charilaos Skandylas. Compositional Security Analysis of Dynamic Component-based Systems. ASE '24: Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering, Pages 1232 – 1244. doi.org/10.1145/3691620.3695499

Sougata Bose, Thomas A. Henzinger, Karoliina Lehtinen, Sven Schewe, Patrick Totzke: History-deterministic Timed Automata. 2024. In Logical Methods in Computer Science, 20(4:1). [doi.org/10.46298/lmcs-20\(4:1\)2024](https://doi.org/10.46298/lmcs-20(4:1)2024)

Narges Khakpour, David Parker. Partially-Observable Security Games for Attack-Defence Analysis in Software Systems, 22nd International Conference on Software Engineering and Formal Methods (SEFM 2024). doi.org/10.1007/978-3-031-77382-2_9

Daniele Dell'Erba, Yong Li, Sven Schewe. DFAMiner: Mining minimal separating DFAs from labelled samples. In Proceedings of the 37th International Symposium on Formal Methods (FM 2024), pp. 48–66, 2024. doi.org/10.48550/arXiv.2405.18871

Ernst Moritz Hahn, Mateo Perez, Sven Schewe, Fabio Somenzi, Ashutosh Trivedi, Dominik Wojtczak: Omega-Regular Decision Processes. In Proc. Thirty-Eighth Conference on Artificial Intelligence (AAAI 2024), pp. 21125–21133, 2024. doi.org/10.1609/aaai.v38i19.30105

Nicolas Berthier and Narges Khakpour. Symbolic Abstract Heaps for Polymorphic Information-Flow Guard Inference. In the 23rd International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2023), 66-90, 2023. doi.org/10.48550/arXiv.2211.03450

Ernst Moritz Hahn, Mateo Perez, Sven Schewe, Fabio Somenzi, Ashutosh Trivedi, and Dominik Wojtczak. Omega-Regular Reward Machines. In Proc. 26th European Conference on Artificial Intelligence (ECAI 2023), pp. 972–979, 2023. doi.org/10.48550/arXiv.2308.07469

Armando Castañeda, Gregory V. Chockler, Brijesh Dongol, Ori Lahav. What Cannot Be Implemented on Weak Memory? DISC 2024: 11:1-11:22. arxiv.org/abs/2405.16611

Eleni Vafeiadi Bila, Brijesh Dongol. A verified durable transactional mutex lock for persistent x86-TSO. Formal Methods Syst. Des. 64(1): 237-282 (2024). doi.org/10.1007/s10703-024-00462-1

Maurice H. ter Beek, Manfred Broy, Brijesh Dongol. The Role of Formal Methods in Computer Science Education. Inroads 15(4): 58-66 (2024). dl.acm.org/doi/10.1145/3702231

Sharar Ahmadi, Brijesh Dongol, Matt Griffin. Operationally proving memory access violations in Isabelle/HOL. Sci. Comput. Program. 234: 103088 (2024). doi.org/10.1016/j.scico.2024.103088

Brijesh Dongol, Matt Griffin, Andrei Popescu, Jamie Wright. Relative Security: Formally Modeling and (Dis)Proving Resilience Against Semantic Optimization Vulnerabilities. CSF 2024: 403-418. ieeexplore.ieee.org/abstract/document/10664336

Azalea Raad, Ori Lahav, John Wickerson, Piotr Balcer, Brijesh Dongol. Intel PMDK Transactions: Specification, Validation and Concurrency. ESOP (2) 2024: 150-179. doi.org/10.48550/arXiv.2312.13828

Azalea Raad, Ori Lahav, John Wickerson, Piotr Balcer, Brijesh Dongol. Artifact Report: Intel PMDK Transactions: Specification, Validation and Concurrency. ESOP (2) 2024: 180-184. doi.org/10.1007/978-3-031-57267-8_7

Lara Bargmann, Brijesh Dongol, Heike Wehrheim. Unifying Weak Memory Verification Using Potentials. FM (1) 2024: 519-537. doi.org/10.1007/978-3-031-71162-6_27

Sergey Egorov, Gregory V. Chockler, Brijesh Dongol, Dan O’Keeffe, Sadegh Keshavarzi. Mangosteen: Fast Transparent Durability for Linearizable Applications using NVM. USENIX ATC 2024: 799-815. dl.acm.org/doi/10.5555/3691992.3692041

Stefan Bodenmüller, John Derrick, Brijesh Dongol, Gerhard Schellhorn, Heike Wehrheim. A Fully Verified Persistency Library. VMCAI (2) 2024: 26-47. link.springer.com/chapter/10.1007/978-3-031-50521-8_2

EQUALITY, DIVERSITY AND INCLUSION

At VeTSS we believe that creative and innovative research needs diversity, inclusion and equality of access, and that as a Research Institute we have a responsibility to identify and remove current barriers to participation. We are aware of the challenges that still remain for us, but the below is a short review of our efforts and partial successes this year.

SUMMER SCHOOL

This year's programme attracted over 50 PhD students and early-career researchers from universities across the United Kingdom. We're particularly proud that 30% of our participants (including lecturers) were women, reflecting our commitment to fostering diversity in computer science research. We continue to offer free registration and accommodation and have been able to offer partial travel support grants to make sure that the Summer School is accessible to all.

ANNUAL CONFERENCE

This year's programme welcomed over 100 delegates from universities and industries across the United Kingdom. Our speakers and attendees reflected a diverse range of participants, with strong contributions from under-represented communities. We are continuously working to open the communication channels to circulate details of our calls and invitations to our events to the largest number of people.

FORMAL SPECIFICATION AND VALIDATION AT SCALE

This year's programme attracted over 100 delegates from universities and industries across Europe and the United States. Of these, 75 delegates attended the workshop in person, while the others joined virtually. Participants and speakers represented different communities in academia, industry and government across a range of career levels, with women making up 30% of the total attendees.



THE RESEARCH INSTITUTE ON VERIFIED
TRUSTWORTHY SOFTWARE SYSTEMS

CONTACT US

vetss.org.uk

contact@vetss.org.uk

in [linkedin.com/in/VeTSS/](https://www.linkedin.com/in/VeTSS/)



IMPERIAL