RESEARCH INSTITUTE IN
VERIFIED TRUSTWORTHY SOFTWARE SYSTEMS

Fifth Workshop on Formal Methods and Tools for Security (FMATS)

21-22 September, Microsoft Research, Cambridge

Programme

Morning of Thursday, 21st September 2017

9:30-10:15 Registration with Tea and Coffee

10:15-10:20 Welcome by **Philippa Gardner** (Imperial College London, Director of VeTSS) and **Andy Gordon** (Principal Researcher at MSR Cambridge)

10:20-11:00 **Peter O'Hearn** (Facebook London / UCL)
Principles and Practice of Interprocedural Reasoning at Scale.

Peter O'Hearn is a principal engineer at Facebook and leader of the team working on the Facebook Infer verification tool. Together with Reynolds, he is the creator of separation logic, used for analysing C and Java programs.

11:00-11:30 **Daniel Kroening** (Oxford / DiffBlue)

Daniel Kroening is the creator of CBMC, a bounded model checker for C and Java. He is also the founder of Diffblue, $22M series A funding.

11:35-12:00 Tea and Coffee

12:00-12:30 **Alastair Donaldson** (Imperial College)
Industrial-strength analysis and testing tools for multicore programming

Alastair Donaldson has an EPSRC Early Career Fellowship and has won the 2017 BCS Roger Needham (mid-career) Award for computer science and engineering as well as the Best paper award at FSE 2017, with Tyler Sorensen and Hugues Evrard. He is a Co-I on the VeTSS funded project: Automated Testing for Web Browsers.

12:30-13:00 Short talks for PhD Students, RAs and industrialists

13:00-14:00 Lunch

Afternoon of Thursday, 21st September 2017

14:00-14:30 **Neil White** (Altran UK)

Neil White is head of engineering at Altran UK. His company has developed a fully specified and verified software for UK air-traffic control.

14:30-15:00 **Nathan Chong** (ARM)
Reasoning about Transactional Memory, Axiomatically

Nathan Chong is a Staff Researcher at Arm in the Security and Correctness Group. He works on specification and verification at the hardware/software boundary, including low-level systems code and architecture. Nathan has a PhD from Imperial College and was overall winner of the EPSRC ICT Pioneers competition in 2014.

15:00-15:30 Short talks for PhD Students, RAs and industrialists

15:30-16:00 Tea and Coffee break

16:00-16:30 **Boris Köpf** (IMDEA, Madrid)
Static Quantification of Timing Side Channels

Boris Köpf is an associate research professor at the IMDEA Software Institute in Madrid, Spain. His research focuses on side-channel attacks (and countermeasures) and privacy-preserving data publishing.

16:30-17:00 **Antoine Delignat-Lavaud** (Microsoft Research)
Deploying cryptographically-verified components for the HTTPS ecosystem

Antoine Delignat-Lavaud is a researcher at Microsoft. He is part of Project Everest, which aims to build and deploy a verified HTTPS stack.

17:00-17:30 Discussion: VeTSS: Analysis and Verification in the Industrial Software Design Process

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

Westminster College Hall is on Madingley Road, Cambridge, CB3 0AA. This is a 30-minute walk or a 15-minute taxi ride from the venue. Taxis can be booked from the local taxi firm Panther Taxis on 01223 715715/ 424424/ 523523. Please note that there is very limited car parking at Westminster College.

Morning of Friday, 22nd September 2017

9:00-9:30 Tea and Coffee

9:30-10:00 **Sylvan Clebsch** (Microsoft Research)
Coco Framework for enterprise Blockchain networks

Sylvan Clebsch is a principal research software development engineer at Microsoft Research. He will talk about the Coco Framework, to improve performance, confidentiality and governance characteristics of enterprise blockchain networks, which is raising some interesting formal methods challenges.

10:00-10:30 **Scott Owens** (Kent, VeTSS'17)
Building Trustworthy Software with CakeML

Scott Owens is part of the the team that has developed the functional programming language, Cake ML, with a proven-correct compiler and runtime system. He is the lead

researcher on the VeTSS-funded project Verifying Efficient Libraries in CakeML. Ramana Kumar received this year's ACM John C. Reynolds Doctoral Dissertation Award for his PhD thesis on Cake ML.

10:30-10:45 **Greta Yorsh** (Queen Mary, VeTSS'17)
Unbounded Superoptimization

Greta Yorsh was previously a software engineer at ARM, developing open-source compilation tools, and a researcher at IBM Watson, New York. She is the lead researcher on the VeTSS-funded project Supervectorizer.

10:45-11:15 Tea and Coffee

11:15-11:45 **James Cheney** (Edinburgh, VeTSS'17)
Intersection between databases and programming languages

James Cheney is the recipient of an ERC Consolidator Grant to develop Skye, a programming language bridging theory and practice for scientific data curation. He is the co-lead on the VeTSS-funded project Mechanising the Metatheory of SQL with Nulls, together with Wilmer Ricciotti.

11:45-12:00 **Johannes Kinder** (Royal Holloway, VeTSS'17)
Automated security testing for JavaScript

Johannes Kinder is the lead researcher on the VeTSS-funded project EASTEND, and will talk about the assessment and improvement of the reliability and security of software using automated analysis tools, integrating ideas from programming languages, software engineering and systems security.

12:00-12:15 **Conrad Watt** (Cambridge)
Formalising WebAssembly

Conrad Watt is a PhD student at Cambridge University supervised by Peter Sewell. He is currently focussed on formalising the WebAssembly language and its related artefacts, in particular the SharedArrayBuffer proposal.

12.15-12.30 **Simon Foster** (York, VeTSS'17)
Isabelle/UTP: A Verification Toolbox for Unifying Theories

Simon Foster is a Postdoctoral Research Fellow at the University of York working on the EU H2020 project "INTO-CPS" where he researches formal semantics and theorem proving for cyber-physical systems. He is co-investigator on VeTSS funded project "Mechanised Assume-Guarantee Reasoning for Control Law Diagrams via Circus".

12.30-12.45 **Kyndylan Nienhuis** (Cambridge)
Security proofs of the CHERI ISA in Isabelle

Kyndylan Nienhuis is a PhD student and Gates scholar at the University of Cambridge.

12.45-14.00 Lunch

Afternoon of Friday, 22nd September 2017

14:00-14:30 **Rod Chapman** (Protean Code Ltd.)
Sanitising Sensitive Data: How to get it Right (or at least Less Wrong…)

Rod Chapman, representing Protean Code Ltd., was formerly a principal engineer with Altran UK. Rod specialises in the design process and technologies used in the development of security-critical and safety-critical systems.

14:30-15:00 **David Clark** (UCL, former RI2 institute (RIAPAV))
Indexing Operators to Extend the Reach of Symbolic Execution

David Clark's research interests include program flow security, slicing programs and software models, malware detection and classification, software testing and application of information theory to software analysis.

15:00-15:30 **Mark Batty** (University of Kent, VeTSS'17)

Mark Batty's research focusses on formal specifications, testing tools and verification techniques for real-world concurrent systems, with an emphasis on established programming language interfaces (e.g. C and C++) and concrete testable artefacts (e.g., weak memory models). He has a Lloyds Register Foundation and RAEng Research Fellowship. In 2015, he won the ACM Sigplan John C. Reynolds Doctoral Dissertation Award and the UK BCS/CPHC Distinguished Dissertation Award.

15:30-16:00 Tea and Coffee break