David Cock

May 25, 2023

Alfred-Comte-Strasse 3
8953 Dietikon
Switzerland

Telephone, mobile: +41 79 897 11 17
Telephone, work: +41 44 632 68 79
david.cock@inf.ethz.ch
davidcock@fastmail.fm
https://people.inf.ethz.ch/dcock/

Employment

7/2017–	*Oberassistent I (Senior Researcher) & Dozent (Lecturer), Institute for Computing Platforms (Systems Group), D-INFK, ETH Zürich*
1/2015–6/2017	*Postdoctoral researcher, Institute for Computing Platforms (Systems Group), D-INFK, ETH Zürich*
2009-2014	*PhD Student, University of New South Wales & National ICT Australia*
2005–2009	*PhD-track Research Engineer, National ICT Australia* L4.verified & seL4 projects, supervisor Gerwin Klein.

Education

2014	*PhD, University of New South Wales & National ICT Australia* "Leakage in Trustworthy Systems", supervisor Gernot Heiser, software systems research group (SSRG).
2004	*BSc (Hons), University of New South Wales* Mathematics & Computer Science, major in Systems and Algebra.

Research

I work at the intersection of systems software (in particular operating systems), formal methods (practical software verification), and computer architecture (novel and reconfigurable platforms), with particular focus on the correct, trustworthy, and high-performance interaction between systems software and the hardware.
I was a founding member of the seL4[1] and L4.verified[2] projects (Derrin et al., 2006; Klein et al., 2009, 2010) in 2005, which produced the first fully-verified general-purpose operating system kernel. I was the principal author of the final C implementation, achieving fastest published IPC (inter-process communication) path on the ARM architecture. I was responsible for, or involved with, developing the nondeterministic, monadic refinement framework (Cock et al., 2008), automatic generation and verification of low-level data structures (Winwood et al., 2009; Cock, 2008), and our hybrid ARM ISA simulator (Cock, 2010).
My Ph.D. work (Cock, 2014a) extended the analysis of seL4 to non-functional properties, particularly side-channels (Cock, 2011, 2013, 2014b) and verification of probabilistic properties more generally (Cock, 2012). The empirical techniques I developed began a continuing and independent line of research at UNSW (Cock et al., 2014; Ge et al., 2018), which has continued beyond my graduation.
Since 2016 I have lead the Enzian[3] project at ETHZ. I was responsible for the design and production of a 2-socket server system incorporating a 48-core server CPU and large FPGA linked by the CPU's native coherent interconnect. In addition to overall design and project management, I managed subcontractor relationships (including a public tender), purchasing, and project scheduling. I was personally involved in design and implementation at all levels, including the low-level FPGA protocol stack, CPU firmware, PCB design and review, production test planning and implementation, and compute cluster design and management (Cock et al., 2022).

[1] https://trustworthy.systems/projects/TS/l4.verified/
[2] https://trustworthy.systems/projects/seL4/
[3] http://enzian.systems/

My ongoing work also includes establishing a formally trustworthy, yet precise model of the hardware software interface (Achermann et al., 2017, 2018), both by formal modelling and real-time verification using hardware trace data. My foundational formal work in this area forms the basis of an extensive, ongoing research agenda at ETHZ (Achermann et al., 2021b; Fiedler et al., 2023).

Key Publications

- Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. seL4: Formal verification of an OS kernel. In *Proceedings of the 22nd ACM Symposium on Operating Systems Principles*, pages 207–220. ACM, October 2009. doi:10.1145/1629575.1629596
- David Cock, Qian Ge, Toby Murray, and Gernot Heiser. The last mile: An empirical study of timing channels on seL4. In *Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security*, pages 570–581. ACM, November 2014. doi:10.1145/2660267.2660294
- Reto Achermann, David Cock, Roni Haecki, Nora Hossle, Lukas Humbel, Timothy Roscoe, and Daniel Schwyn. mmapx: Uniform memory protection in a heterogeneous world. In *Proceedings of the 18th Workshop on Hot Topics in Operating Systems*, page 159–166. ACM, June 2021b. doi:10.1145/3458336.3465273
- David Cock, Abishek Ramdas, Daniel Schwyn, Michael Giardino, Adam Turowski, Zhenhao He, Nora Hossle, Dario Korolija, Melissa Licciardello, Kristina Martsenko, Reto Achermann, Gustavo Alonso, and Timothy Roscoe. Enzian: An open, general, CPU/FPGA platform for systems software research. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, page 434–451. ACM, 2022. doi:10.1145/3503222.3507742

Teaching

2018– *Lecturer in Charge, Informal Methods, ETH Zürich*

Formal methods are increasingly a key part of the methodological toolkit of systems programmers - those writing operating systems, databases, and distributed systems. This course is about how to apply concepts, techniques, and principles from formal methods to such software systems, and how to get into the habit of thinking formally about systems design even when writing low-level C code.

2015– *Lecturer, Advanced Operating Systems, ETH Zürich*

This is a Masters-level capstone course in the Systems curriculum at ETH, based on the UNSW model.

2009–2014 *Teaching Assistant, Operating Systems and Advanced Operating Systems, UNSW*

Small-group instruction of both undergraduate and postgraduate students, and marking duties. Individual guidance and assessment for advanced student projects.

Industrial Experience

2005–2014 *Computer Support Officer, National ICT Australia.*

Technical and performance-optimisation support for the automated regression testing of large mechanised proofs. Resource planning and equipment acquisition.

2003–2005 *Programmer, Brain Resource Pty. Ltd.*

Clinical electroencephalogram acquisition system development in Python and C, on a customised Debian distribution, deployed worldwide.

Grants & Awards

2022 *ACM Software Systems Award*

seL4. Jointly, for the development of the first industrial-strength, high-performance operating system to have been the subject of a complete, mechanically checked proof of full functional correctness.

2019 *ACM SIGOPS Hall of Fame Award*

"seL4: Formal Verification of an OS Kernel" (Klein et al., 2009)

2014 *CISRA Best Research Paper Award (UNSW)*

"The Last Mile: An Empirical Study of Timing Channels on seL4" (Cock et al., 2014)

2009–2013 *Australian Postgraduate Award*

A competitive federally-funded full scholarship for research students.

2009–2013 *NICTA Research Project Award*

A competitive scholarship for students undertaking project work at NICTA.

2009–2013 *UNSW Engineering Top-Up Scholarship*

Limited numbers offered annually, awarded for teaching work.

Scientific Engagement and PC Membership

- ACM—Journal of the ACM; EMSOFT PC 2019-2021; PLOS PC 2023; Eurosys PC 2024.
- USENIX—ATC PC 2019, 2021-2023.
- IEEE—RTAS PC 2020.
- Elsevier—Science of Computer Programming.
- Springer—Design Automation for Embedded Systems, European Symposium on Programming; International Symposium on Formal Methods, Security Proofs for Embedded Systems; International Symposium on Automated Technology for Verification and Analysis.

References

Timothy Roscoe
Professor, Department of Computer Science, ETH Zürich
Telephone: +41 44 632 88 40
troscoe@inf.ethz.ch
https://people.inf.ethz.ch/troscoe/

Gustavo Alonso
Professor, Department of Computer Science, ETH Zürich
Telephone: +41 44 632 73 06
alonso@inf.ethz.ch
https://people.inf.ethz.ch/alonso/

Gernot Heiser
Professor, School of Computer Science and Engineering,
UNSW Sydney
Telephone: +61 2 9065 5346
gernot@unsw.edu.au
https://gernot-heiser.org/

Gerwin Klein
Conjoint Professor, School of Computer Science and Engineering,
UNSW Sydney
Founder and Chief Scientist at Proofcraft
kleing@unsw.edu.au
https://proofcraft.systems/

Full Publication List

Reto Achermann, Lukas Humbel, David Cock, and Timothy Roscoe. Formalizing memory accesses and interrupts. In Holger Hermanns and Peter Höfner, editors, *Proceedings of the 2nd Workshop on Models for Formal Analysis of Real Systems*, volume 244 of *Electronic Proceedings in Theoretical Computer Science*, pages 66–116. Open Publishing Association, April 2017. doi:10.4204/EPTCS.244.4.

Reto Achermann, Lukas Humbel, David Cock, and Timothy Roscoe. Physical addressing on real hardware in Isabelle/HOL. In Jeremy Avigad and Assia Mahboubi, editors, *Proceedings of the 9th International Conference on Interactive Theorem Proving*, volume 10895 of *Lecture Notes in Computer Science*, pages 1–19. Springer, July 2018. doi:10.1007/978-3-319-94821-8_1.

Reto Achermann, Nora Hossle, Lukas Humbel, Daniel Schwyn, David Cock, and Timothy Roscoe. A least-privilege memory protection model for modern hardware. 2019. doi:10.48550/ARXIV.1908.08707. eprint.

Reto Achermann, David Cock, Roni Haecki, Nora Hossle, Lukas Humbel, Timothy Roscoe, and Daniel Schwyn. Generating correct initial page tables from formal hardware descriptions. In *Proceedings of the 11th Workshop on Programming Languages and Operating Systems*, page 69–75. ACM, October 2021a. doi:10.1145/3477113.3487270.

Reto Achermann, David Cock, Roni Haecki, Nora Hossle, Lukas Humbel, Timothy Roscoe, and Daniel Schwyn. mmapx: Uniform memory protection in a heterogeneous world. In *Proceedings of the 18th Workshop on Hot Topics in Operating Systems*, page 159–166. ACM, June 2021b. doi:10.1145/3458336.3465273.

Gustavo Alonso, Timothy Roscoe, David Cock, Mohsen Ewaida, Kaan Kara, Dario Korolija, David Sidler, and Zeke Wang. Tackling hardware/software co-design from a database perspective. In *Proceedings of the 10th Conference on Innovative Data Systems Research*, January 2020. doi:10.3929/ethz-b-000456368.

David Cock. Bitfields and tagged unions in C: Verification through automatic generation. In Bernhard Beckert and Gerwin Klein, editors, *Proceedings of the 5th International Verification Workshop*, volume 372 of *CEUR Workshop Proceedings*, pages 44–55, August 2008. URL `http://ceur-ws.org/Vol-372/paper06.pdf`.

David Cock. Lyrebird – assigning meanings to machines. In Gerwin Klein, Ralf Huuck, and Bastian Schlich, editors, *Proceedings of the 5th International Conference on Systems Software Verification*, pages 1–9. USENIX, October 2010. URL `https://www.usenix.org/legacy/events/ssv10/tech/full_papers/Cock.pdf`.

David Cock. Exploitation as an inference problem. In *Proceedings of the 4th ACM Workshop on Artificial Intelligence and Security*, pages 105–106. ACM, October 2011. doi:10.1145/2046684.2046702.

David Cock. Verifying probabilistic correctness in Isabelle with pGCL. In *Proceedings of the 7th International Conference on Systems Software Verification*, volume 102 of *Electronic Proceedings in Theoretical Computer Science*, pages 167–176. Open Publishing Association, November 2012. doi:10.4204/EPTCS.102.15.

David Cock. Practical probability: Applying pGCL to lattice scheduling. In *Proceedings of the 4th International Conference on Interactive Theorem Proving*, volume 7998 of *Lecture Notes in Computer Science*, pages 311–327, Rennes, France, July 2013. Springer. doi:10.1007/978-3-642-39634-2_23.

David Cock. *Leakage in Trustworthy Systems*. PhD thesis, UNSW Computer Science and Engineering, Sydney, Australia, August 2014a. `https://doi.org/10.26190/unsworks/16942`.

David Cock. From probabilistic operational semantics to information theory - side channels with pGCL in Isabelle. In *Proceedings of the 5th International Conference on Interactive Theorem Proving*, volume 8558 of *Lecture Notes in Computer Science*, pages 177–192, Vienna, Austria, July 2014b. Springer. doi:10.1007/978-3-319-08970-6_12.

David Cock. pGCL for Isabelle. *Archive of Formal Proofs*, July 2014c. `http://isa-afp.org/entries/pGCL.shtml`, Formal proof development.

David Cock, Gerwin Klein, and Thomas Sewell. Secure microkernels, state monads and scalable refinement. In Otmane Ait Mohamed, César Muñoz, and Sofiène Tahar, editors, *Proceedings of the 21st International Conference on Theorem Proving in Higher Order Logics*, volume 5170 of *Lecture Notes in Computer Science*, pages 167–182. Springer, August 2008. doi:10.1007/978-3-540-71067-7_16.

David Cock, Qian Ge, Toby Murray, and Gernot Heiser. The last mile: An empirical study of timing channels on seL4. In *Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security*, pages 570–581. ACM, November 2014. doi:10.1145/2660267.2660294.

David Cock, Abishek Ramdas, Daniel Schwyn, Michael Giardino, Adam Turowski, Zhenhao He, Nora Hossle, Dario Korolija, Melissa Licciardello, Kristina Martsenko, Reto Achermann, Gustavo Alonso, and Timothy Roscoe. Enzian: An open, general, CPU/FPGA platform for systems software research. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, page 434–451. ACM, 2022. doi:10.1145/3503222.3507742.

Philip Derrin, Kevin Elphinstone, Gerwin Klein, David Cock, and Manuel M. T. Chakravarty. Running the manual: An approach to high-assurance microkernel development. In *Proceedings of the ACM SIGPLAN Haskell Workshop*, September 2006. doi:10.1145/1159842.1159850.

Ben Fiedler, Daniel Schwyn, Constantin Gierczak-Galle, David Cock, and Timothy Roscoe. Putting out the hardware dumpster fire. In *Proceedings of the 20th Workshop on Hot Topics in Operating Systems*. ACM, June 2023. To appear.

Qian Ge, Yuval Yarom, David Cock, and Gernot Heiser. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *Journal of Cryptographic Engineering*, 8(1):1–27, 2018. doi:10.1007/s13389-016-0141-6.

Roni Haecki, Lukas Humbel, Reto Achermann, David Cock, Daniel Schwyn, and Timothy Roscoe. CleanQ: a lightweight, uniform, formally specified interface for intra-machine data transfer. 2019. doi:10.48550/ARXIV.1911.08773. eprint.

Lukas Humbel, Daniel Schwyn, Nora Hossle, Roni Haecki, Melissa Licciardello, Jan Schaer, David Cock, Michael Giardino, and Timothy Roscoe. A model-checked I2C specification. In Alfons Laarman and Ana Sokolova, editors, *Proceedings of the 27th International SPIN Symposium on Model Checking of Software*, pages 177–193. Springer, 2021. doi:10.1007/978-3-030-84629-9_10.

Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. seL4: Formal verification of an OS kernel. In *Proceedings of the 22nd ACM Symposium on Operating Systems Principles*, pages 207–220. ACM, October 2009. doi:10.1145/1629575.1629596.

Gerwin Klein, June Andronick, Kevin Elphinstone, Gernot Heiser, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. seL4: Formal verification of an operating system kernel. *Communications of the ACM*, 53(6):107–115, June 2010. doi:10.1145/1743546.1743574.

Jasmin Schult, Daniel Schwyn, Michael Giardino, David Cock, Reto Achermann, and Timothy Roscoe. Declarative power sequencing. *ACM Transactions on Embedded Computing Systems*, 20(5s), September 2021. doi:10.1145/3477039.

Simon Winwood, Gerwin Klein, Thomas Sewell, June Andronick, David Cock, and Michael Norrish. Mind the gap: A verification framework for low-level C. In Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel, editors, *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics*, volume 5674 of *Lecture Notes in Computer Science*, pages 500–515, Munich, Germany, August 2009. Springer. doi:10.1007/978-3-642-03359-9_34.