Prof. Dr. Gidon Marian Ernst

April 1, 2019

Software Verification, Software and Computational Systems Lab
Ludwig-Maximilians-Universität München
www.sosy-lab.org/people/ernst gidon.ernst@sosy.ifi.lmu.de +49 89 2180 9376

Research Interest

- Compositional specification and proof methods for nonstandard correctness properties
- Development of correct software and systems in the large with formal methods
- Building and comparing software tools for program analysis

Education

2010–2016	Dr. rer. nat, Formal Methods, Augsburg University (**summa cum laude**) Prof. Wolfgang Reif, Prof. Alexander Knapp, Prof. John Derrick
2008–2010	MSc with honours, Software Engineering, Augsburg University (1.15)
2005–2008	BSc, Informatik, Freiburg University (1.3)

Positions

since 2019	Junior Professor for Software Verification, LMU Munich
2018–2019	Postdoc Fellow, University of Melbourne, Dr. Toby Murray
2017–2018	Postdoc Researcher, National Institute of Informatics, Tokyo, Prof. Ichiro Hasuo
2017	Intern, Amazon New York, Prof. Byron Cook
2010–2016	Research Assistant, Augsburg University, Prof. Wolfgang Reif
2008–2010	Student Researcher, Augsburg University, Prof. Wolfgang Reif
2009	Intern, Siemens Corporate Technology, Munich

Visits

2018	University of Waterloo, Canada, Prof. Krzysztof Czarnecki, Prof. Sean Sedwards

Research & Projects

- COVERN: Compositional verification of noninterference (PI: T. Murray, covern.org)
- FalStar: Model based testing of hybrid systems (PI: I. Hasuo, github.com/ERATOMMSD/falstar)
- Flashix: A verified POSIX compliant flash file system (PI: W. Reif, isse.de/flashix)
- KIV: A tool for formal systems development and interactive verification (isse.de/kiv)
- Integration of Shape Analysis und Theorem Proving (github.com/gernst/IMP3)
- TakaTuka Java Virtual Machine for resource constrained devices (takatuka.sourceforge.net)

Awards

- VerifyThis @ ETAPS, London, 2015: **best student team** with Jörg Pfähler.
- VerifyThis @ FM, Paris, 2012: **best student team** with Jörg Pfähler.
- 2nd VSCOMP 2011: **gold medal** with Gerhard Schellhorn, Bogdan Tofan, Kurt Stenzel.

Press

- Garantierte Fehlerfreiheit für Flash-Speicher, Augsburger Allgemeine, Forschungsmagazin, 2016. (Guaranteed bug-freedom for flash memory, research magazine of Augsburger Allgemeine).

Professional Activities

Co-Organizer

- Workshop on Formal Techniques for Java-like Programs (FTfJP), 2019.
- ARCH friendly competition, falsification category, 2019.
- VerifyThis Software Verification Competition, 2018.

Programm Commitee

- Symposium on Formal Approaches to Parallel and Distributed Systems (4PAD), 2019.
- Symposium On Applied Computing (SAC), track: Software Verification and Testing, 2019.
- Symposium on Formal Approaches to Parallel and Distributed Systems (4PAD), 2018.
- Workshop on Automated Reasoning in Software Verification (ARiSVe), 2013.

Artifact Evaluation Comitee

- Static Analysis Symposium (SAS), 2018.

Journal Reviewer

- Journal of Logical and Algebraic Methods in Programming (JLAMP), 2016, 2018, 2019.
- Computing Science—Research and Education (CORE), 2018.
- Software and Systems Modeling (SoSyM), 2018.
- Formal Aspects of Computing (FAC), 2015, 2017.
- Science of Computer Programming (SCP), 2014.
- Software Tools for Technology Transfer (STTT), 2013.

Conference Reviewer

- Integrated Formal Methods (iFM), 2018.
- Conference on Concurrency Theory (CONCUR), 2018.
- Hybrid Systems: Computation and Control (HSCC), 2017.
- Alloy, ASM, B, TLA, VDM, and Z (ABZ), 2016.
- European Dependable Computing Conference (EDCC), 2012.
- Formal Verification of Object-Oriented Software (FoVeOOS), 2011.
- Tests and Proofs (TAP), 2011.

University Service

- Co-authored proposal for DFG grant RE828/13-2 (PI: W. Reif)
- Representation of the Software-Engineering Elite Graduate Program at the annual VHK career forum, Garching, Germany (2011–2014)
- Conception of the curriculum of the new Bachelor programme Ingenieurinformatik at Augsburg University, commitee member
- User requirements and planning of a new building Materials Resource Management at Augsburg University, commitee member

Teaching

- Formal methods in software engineering lab course (master level, 2010–2016)
- Seminar on systems modeling and verification (master level, 2010-2014)
- Seminar on software and systems engineering (2015)
- Seminar on innovative software engineering concepts (2010–2013)
- PhD supervision: Dongge Liu (with Toby Murray, Ben Rubinstein, 2018–).
- Diploma/Master theses: Stefan Bodenmüller (2016), Berthold Stoll (2013), Michael Pini (2013), Than Son Do (2012).
- Bachelor theses: Lilli Schmidt (2016), Stefan Fritsch (2015), Alexander Vogelsgsang (2015), Stefan Bodenmüller (2014), Klaus Weber (2014), Daniel Halke (2014), Mike Knebel (2013).
- Semester projects: Jessica Ertel (2016), Andreas Sabitzer (2014), Sarah Edenhofer (2013), Jessica Tretter (2013).

Publications

Doctoral Thesis

- G. Ernst. *A Verified POSIX-Compliant Flash File System—Modular Verification Technology & Crash Tolerance*. PhD thesis, Augsburg University, 2016.

Journal Articles

1. Z. Zhang, G. Ernst, S. Sedwards, P. Arcaini, and I. Hasuo. Two-Layered Falsification of Hybrid Systems Guided by Monte Carlo Tree Search. *Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 37(11):2894–2905, 2018.
2. Y. Bao, G. T. Leavens, and G. Ernst. Unifying separation logic and region logic to allow interoperability. *Formal Aspects of Computing*, 30(3–4):381–441, 2018.
3. G. Schellhorn, G. Ernst, J. Pfähler, S. Bodenmüller, and W. Reif. Symbolic execution for a clash-free subset of ASMs. *Science of Computer Programming (SCP)*, 158:21–40, 2018.
4. G. Ernst, J. Pfähler, G. Schellhorn, and W. Reif. Modular, crash-safe refinement for ASMs with submachines. *Science of Computer Programming (SCP)*, 131:3–21, 2016.
5. G. Ernst, J. Pfähler, G. Schellhorn, D. Haneberg, and W. Reif. KIV—Overview and VerifyThis competition. *Software Tools for Technology Transfer (STTT)*, 17(6):677–694, 2015.
6. G. Schellhorn, B. Tofan, G. Ernst, J. Pfähler, and W. Reif. RGITL: A temporal logic framework for compositional reasoning about interleaved programs. *Annals of Mathematics and Artificial Intelligence (AMAI)*, 71:1–44, 2014.
7. G. Ernst, G. Schellhorn, and W. Reif. Verification of B^+ trees by integration of shape analysis and interactive theorem proving. *Software & Systems Modeling (SOSYM)*, 14(1):27–44, 2015.

In Conference/Workshop Proceedings

1. G. Ernst, M. Huisman, W. Mostowski, and M. Ulbrich. VerifyThis – Verification Competition with a Human Factor. In *Proc. of Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 11429 of *LNCS*. Springer, 2019. To appear.
2. A. Dokhanchi, S. Yaghoubi, B. Hoxha, G. Fainekos, G. Ernst, Z. Zhang, P. Arcaini, I. Hasuo, and S. Sedwards. ARCH-COMP18 Category Report: Results on the Falsification Benchmarks. In *Proc. of Applied Verification of Continuous and Hybrid Systems (ARCH)*, volume 54 of *EPiC*, pages 104–109. EasyChair, 2018.
3. G. Ernst, I. Hasuo, Z. Zhang, and S. Sedwards. Time-staging Enhancement of Hybrid System Falsification. In *Proc. of Symbolic and Numerical Methods for Reachability Analysis (SNR)*, EPTCS. 2018.
4. J. Pfähler, G. Ernst, S. Bodenmüller, G. Schellhorn, and W. Reif. Modular verification of order-preserving writeback caches. In *Proc. of Integrated Formal Methods (iFM)*, volume 10510 of *LNCS*, pages 375–390. Springer, 2017.
5. G. Schellhorn, G. Ernst, J. Pfähler, and W. Reif. A relational encoding for a clash-free subset of ASMs. In *Proc. of Alloy, ASM, B, TLA, VDM, and Z (ABZ)*, volume 9675 of *LNCS*, pages 237–243. Springer, 2016.
6. G. Ernst, J. Pfähler, G. Schellhorn, and W. Reif. Inside a verified Flash file system: transactions & garbage collection. In *Proc. of Verified Software: Theories, Tools, Experiments (VSTTE)*, volume 9593 of *LNCS*, pages 73–93. Springer, 2015.
7. Y. Bao, G. T. Leavens, and G. Ernst. Conditional effects in fine-grained region logic. In *Proc. of Formal Techniques for Java-like Programs (FTfJP)*. ACM, 2015.
8. G. Ernst, J. Pfähler, G. Schellhorn, and W. Reif. Modular refinement for submachines of ASMs. In *Proc. of Alloy, ASM, B, TLA, VDM, and Z (ABZ)*, volume 8477 of *LNCS*, pages 188–203. Springer, 2014.

9. G. Schellhorn, G. Ernst, J. Pfähler, D. Haneberg, and W. Reif. Development of a verified Flash file system. In *Proc. of Alloy, ASM, B, TLA, VDM, and Z (ABZ)*, volume 8477 of *LNCS*, pages 9–24. Springer, 2014. Invited Paper.
10. G. Ernst, G. Schellhorn, D. Haneberg, J. Pfähler, and W. Reif. Verification of a Virtual Filesystem Switch. In *Proc. of Verified Software: Theories, Tools, Experiments (VSTTE)*, volume 8164 of *LNCS*, pages 242–261. Springer, 2013.
11. Tofan B, G. Schellhorn, Gidon G. Ernst, J. Pfähler, and W. Reif. Compositional verification of a lock-free stack with RGITL. *Electronic Communications of the Automated Verification of Critical Systems (EASST)*, 66, 2014.
12. J. Pfähler, G. Ernst, G. Schellhorn, D. Haneberg, and W. Reif. Formal specification of an erase block management layer for Flash memory. In *Haifa Verification Conference (HVC)*, volume 8244 of *LNCS*, pages 214–229. Springer, 2013.
13. G. Ernst, G. Schellhorn, D. Haneberg, J. Pfähler, and W. Reif. A formal model of a Virtual Filesystem Switch. In *Proc. of Software and Systems Modeling (SSV)*, volume 102 of *EPTCS*, pages 33–45, 2012.
14. G. Ernst, G. Schellhorn, and W. Reif. Verification of B^+ trees: an experiment combining shape analysis and interactive theorem proving. In *Proc. of Software Engineering and Formal Methods (SEFM)*, volume 7041 of *LNCS*, pages 188–203. Springer, 2011.
15. G. Schellhorn, B. Tofan, G. Ernst, and W. Reif. Interleaved programs and rely-guarantee reasoning with ITL. In *Proc. of Temporal Representation and Reasoning (TIME)*, pages 99–106. IEEE, 2011.
16. M. Junker, D. Haneberg, G. Schellhorn, W. Reif, and G. Ernst. Simulating a Flash File System with CoreASM and Eclipse. In *Proc. of Dependable Software for Critical Infrastructures (DSCI)*, volume 192 of *GI Lecture Notes in Informatics*. Gesellschaft für Informatik, 2011.
17. T. Bormer, M. Brockschmidt, D. Distefano, G. Ernst, J.-C. Filliâtre, R. Grigore, M. Huisman, V. Klebanov, C. Marché, R. Monahan, W. Mostowski, N. Polikarpova, C. Scheben, G. Schellhorn, B. Tofan, J. Tschannen, and M. Ulbrich. The COST IC0701 verification competition 2011. In *Proc. of Formal Verification of Object-Oriented Software (FoVeOOS)*, volume 7421 of *LNCS*, pages 3–21. Springer, 2011.
18. F. Aslam, L. Fennell, C. Schindelhauer, P. Thiemann, G. Ernst, E. Haussmann, S. Rührup, and Z. A. Uzmi. Optimized Java binary and virtual machine for tiny motes. In *Proc. of Distributed Computing in Sensor Systems (DCOSS)*, volume 6131 of *LNCS*, pages 15–30. Springer, 2010.

Other

1. M. Huisman, R. Monahan, P. Müller, A. Paskevich, and G. Ernst. VerifyThis 2018: A Program Verification Competition. Technical Report hal-01981937, Université Paris-Saclay, 2018.
2. G. Ernst A. Issa, T. Murray. In Search of Perfect Users: Towards Understanding the Usability of Converged Multi-Level Secure User Interfaces. In *Proc. of Computer Human Interaction Australia (OzCHI)*. 2018. Work in Progress Report.
3. Z. Zhang, G. Ernst, I. Hasuo, and S. Sedwards. Time-staging Enhancement of Hybrid System Falsification (Abstract). In *Proc. of Monitoring and Testing of Cyber-Physical Systems (MT-CPS)*. IEEE, 2018.
4. Y. Bao, G. T. Leavens, and G. Ernst. Translating separation logic into dynamic frames using fine-grained region logic. Technical Report CS-TR-13-02a, University of Central Florida, 2014.
5. J. Pfähler, G. Ernst, G. Schellhorn, D. Haneberg, and W. Reif. Crash-safe refinement for a verified Flash file system. Technical Report 2014-02, University of Augsburg, 2014.
6. G. Ernst and A. Habermaier. Garantiert fehlerfrei! *Mechatroniknews*, Februar 2013.
7. F. Aslam, C. Schindelhauer, G. Ernst, D. Spyra, J. Meyer, and M. Zalloom. Introducing TakaTuka:

a Java Virtual Machine for motes. In *Proc. of the Embedded Network Sensor Systems (SENSYS)*, pages 399–400. ACM, 2008. Poster Abstract.

Invited Talks

- G. Ernst. Hybrid System Falsifiation by Optimization and Tree Search. Generative Software Development lab, University of Waterloo, Canada, 2018.
- G. Ernst. Insights and Future Directions from the Verifcation of a Flash File System. LMU Munich, Germany, 2018.
- G. Ernst. Flashix: A verified, crash-tolerant flash file system. ERATO project colloquium, National Institute of Informatics, Tokyo, Japan, 2017.
- G. Ernst. On modular verification and substitution. Oberseminar Theoretical Computer Science group, LMU Munich, Germany, 2016.
- G. Schellhorn and G. Ernst. KIV–A Mini Tutorial. Seminar on Evaluating Software Verification Systems: Benchmarks and Competitions, Schloss Dagstuhl, Germany, 2014.
- G. Ernst. Solving the VSTTE'12 competition with KIV. COST IC0701 WG meeting, Darmstadt, Germany, 2012.
- G. Ernst. The KIV Tool. Verified Software: Theories, Tools, Experiments (VSTTE), Philadelphia, PA, USA, 2012. Prize talk for winning a gold medal at the 2nd VSCOMP.
- G. Ernst. Verification of B^+ Trees: An Experiment Combining Shape Analysis and Interactive Theorem Proving. COST IC0701 WG meeting, Aalborg, Denmark, 2011.

Other Events Attended

- International Summer School on Information Security and Protection (ISSISP), Canberra, Australia, 2018.
- Seminar on Model-Based Design for Smart Products and Systems: Advanced Capabilities and Challenging Applications, Shonan, Japan, 2017.
- Django Girls Workshop (Coach), Munich, Germany, 2015.
- Seminar on Evaluating Software Verification Systems, Schloss Dagstuhl, Germany, 2014.
- Summer School on Formal Techniques (SSFT), Menlo Park, USA, 2013.
- COST IC0701 working group meetings: Darmstadt, Germany (2012), Aalborg, Denmark (2011), Turin, Italy (2011).

Software Verification Competitions

- VerifyThis Software Verification Competition @ ETAPS, Thessaloniki, Greece, 2018.
- VerifyThis @ ETAPS, Eindhoven, Netherlands, 2016.
- VerifyThis @ ETAPS, London, UK, 2015.
- 4th VSCOMP 2014.
- VerifyThis @ FM, Paris, France, 2012.
- 2nd VSCOMP 2011.
- VerifyThis @ FoVeOOS, Turin, Italy, 2011.

Hybrid Systems Falsification Competitions

- ARCH-COMP 2018–2019.

Personal Information

Born:	7 February 1986, Freiburg im Breisgau, Germany
Nationality:	German
Languages	German (native), English (IELTS 8.5 of 9.0), French (fair), Japanese (beginner)