

# Prof. Dr. Gidon Marian Ernst

October 7, 2020

Software Verification, Software and Computational Systems Lab  
Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 Munich  
[www.sosy-lab.org/people/ernst](http://www.sosy-lab.org/people/ernst) [gidon.ernst@lmu.de](mailto:gidon.ernst@lmu.de)

+49 89 2180 9376

## RESEARCH INTEREST

- Development of correct software and systems in the large with formal methods
- Compositional specification and proof methods for nonstandard correctness properties
- 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, Informatics, 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, Dr. Ernie Cohen  
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 & COLLABORATION

- CUVEÉ: Blending SMT-LIB with Programs and Weakest Preconditions ([github.com/gernst/cuvee](https://github.com/gernst/cuvee))
- SECCSL: Security Concurrent Separation Logic (with T. Murray, [covern.org/secc](https://covern.org/secc)), and  
SECC: A tool for verifying information flow for low-level concurrent code
- Legion: Machine-Learning based vulnerability detection  
(with D. Liu, T. Murray, B. Rubinstein, [github.com/Alan32Liu/Legion](https://github.com/Alan32Liu/Legion))
- FalStar: A tool for model based testing of hybrid systems  
(with Z. Zhang, S. Sedwards, I. Hasuo, [github.com/ERATOMMSD/falstar](https://github.com/ERATOMMSD/falstar))

## Previous

- KIV: A tool for formal systems development and interactive verification ([isse.de/kiv](https://isse.de/kiv))
- Flashix: A verified POSIX compliant flash file system (PI: W. Reif, [isse.de/flashix](https://isse.de/flashix))
- Integration of Shape Analysis und Theorem Proving ([github.com/gernst/IMP3](https://github.com/gernst/IMP3))
- TakaTuka Java Virtual Machine for resource constrained devices  
(with F. Aslam, C. Schindelhauer, [takatuka.sourceforge.net](https://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, Augsburgener Allgemeine, Forschungsmagazin, 2016.  
(Guaranteed bug-freedom for flash memory, research magazine of Augsburgener Allgemeine).

## **PROFESSIONAL ACTIVITIES**

### Co-Organizer

- Alpine Verification Meeting (AVM), 2021.
- Workshop on Formal Techniques for Java-like Programs (FTfJP), 2019.
- ARCH friendly competition, falsification category, 2019/2020.
- VerifyThis Software Verification Competition, 2018.

### Program Committee

- Hybrid Systems: Computation and Control (HSCC), 2021.
- Verified Software: Theories, Tools, Experiments (VSTTE), 2020.
- Symposium On Applied Computing (SAC), track: Software Verification and Testing, 2019, 2020.
- Symposium on Formal Approaches to Parallel and Distributed Systems (4PAD), 2018, 2019.
- Workshop on Automated Reasoning in Software Verification (ARiSve), 2013.

### Artifact Evaluation Committee

- Hybrid Systems: Computation and Control (HSCC), 2020.
- Static Analysis Symposium (SAS), 2018.

### Journal Reviewer

- Transactions on Modeling and Computer Simulation (TOMACS), 2020.
- Special Issue: Fundamental Approaches to Software Engineering (FASE), 2019.
- Software Tools for Technology Transfer (STTT), 2019.
- Software Quality Journal (SQJO), 2019.
- Journal of Logical and Algebraic Methods in Programming (JLAMP), 2016, 2018, 2019.
- Software and Systems Modeling (SoSyM), 2018, 2019.
- Computing Science—Research and Education (CORE), 2018.
- Formal Aspects of Computing (FAC), 2015, 2017.
- Science of Computer Programming (SCP), 2014.
- Software Tools for Technology Transfer (STTT), 2013.

### Conference Reviewer

- Foundations of Software Engineering (ESEC/FSE), 2020.
- Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2019, 2020.
- Formal Modeling and Analysis of Timed Systems (FORMATS), 2019.
- Software Engineering and Formal Methods (SEFM), 2019.
- 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.

## **TEACHING**

### Qualifications

- PROFiL Basisseminar (professional teaching, led by Dr. Andreas Hendrich), LMU Munich, 2019.
- CIS teaching development (led by Dr. Antonette Mendoza), University of Melbourne, 2018.

### LMU Munich

- Lecture Formal Specification and Verification (Bachelor, 2019–2020)

- Lecture Software Engineering (Bachelor, 2019)
- Lecture Introduction to Informatics: Programming & Software Engineering (for students with informatics as a secondary subject, 2019–2020)
- Seminar Software Quality Assurance (Master, 2020)
- Seminar on Deductive Verification (Master, 2019–2020)
- Seminar on Fuzz Testing (Master, 2019)

#### Augsburg University

- Lab Course Formal Methods in Software Engineering (Master, 2010–2016)
- Seminar on Systems Modeling and Verification (Master, 2010–2014)
- Seminar on Software and Systems Engineering (Bachelor, 2015)
- Seminar on Innovative Software Engineering Concepts (Bachelor, 2010–2013)

#### Students

- PhD: Dongge Liu (with Toby Murray, Ben Rubinstein, 2018–).
- Diploma/Master theses: S. Bodenmüller (2016), B. Stoll (2013), M. Pini (2013), T. S. Do (2012).
- Bachelor theses: G. Alexandru (2019), L. Schmidt (2016), S. Fritsch (2015), A. Vogelsang (2015), S. Bodenmüller (2014), K. Weber (2014), D. Halke (2014), M. Knebel (2013).
- Semester projects: B. Pöttinger (2019), J. Blau (2019), J. Ertel (2016), A. Sabitzer (2014), S. Edenhofer (2013), J. Tretter (2013).

#### UNIVERSITY SERVICE

- Host of Public Climate School Lectures, with Students for Future Munich (2019).
- 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, committee member
- User requirements and planning of a new building Materials Resource Management at Augsburg University, committee member

#### PUBLICATIONS

##### Doctoral Thesis

- G. Ernst. A verified posix-compliant flash file system—modular verification technology & crash tolerance. PhD Thesis, Augsburg University, Institute for Software and Systems Engineering, 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. T. Murray D. Liu, G. Ernst and B. Rubinstein.: Legion: Best-first concolic testing. In *Automated Software Engineering (ASE)*. ACM, 2020. To appear.
2. Dongge Liu, Gidon Ernst, Toby Murray, and Benjamin IP Rubinstein. Legion: Best-first concolic testing (competition contribution). In *Proc. of Fundamental Approaches to Software Engineering (FASE)*, pages 545–549, 2020.
3. G. Ernst, S. Sedwards, Z. Zhang, and I. Hasuo. Fast falsification of hybrid systems using probabilistically adaptive input. In *Proc. of Quantitative Evaluation of Systems (QEST)*, volume 11785 of LNCS, pages 165–181. Springer, 2019.
4. G. Ernst and T. Murray. SecCSL: Security Concurrent Separation Logic. In *Proc. of Computer Aided Verification (CAV)*, volume 11562 of LNCS, pages 208–230. Springer, 2019.
5. G. Ernst, P. Arcaini, A. Donze, G. Fainekos, L. Mathesen, G. Pedrielli, S. Yaghoubi, Y. Yamagata, and Z. Zhang. ARCH-COMP19 Category Report: Results on the Falsification Benchmarks. In *Proc. of Applied Verification of Continuous and Hybrid Systems (ARCH)*, volume 61 of EPiC, pages 129–140. EasyChair, 2019.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. Tofan B, G. Schellhorn, 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.
  17. 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.
  18. 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.
  19. 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.
  20. 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.
  21. 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.
  22. 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.
  23. F. Aslam, L. Fennell, C. Schindelhauer, P. Thiemann, G. Ernst, E. Hausmann, 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. Gidon Ernst and Lukas Rieger. Information Flow Testing of a PGP Keyserver. In *Proc. of VerifyThis Long-term Challenge 2020*, pages 11–13. KIT Library, 2020.
2. Gidon Ernst, Toby Murray, and Mukesh Tiwari. Verifying the Security of a PGP Keyserver. In *Proc. of VerifyThis Long-term Challenge 2020*, pages 14–16. KIT Library, 2020.
3. 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.
4. A. Issa, T. Murray, and G. Ernst. In Search of Perfect Users: Towards Understanding the Usability of Converged Multi-Level Secure User Interfaces. In *Proc. of Computer Human Interaction Australia (OzCHI)*, pages 572–576. ACM, 2018. Work in Progress Report.
5. 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.
6. 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.
7. 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.
8. G. Ernst and A. Habermaier. Garantiert fehlerfrei! *Mechatroniknews*, Februar 2013.
9. 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. Verification of Loops with Invariants and Summaries. CPAchecker Workshop, 2020.
- G. Ernst. VerifyThis tasks in the SV-COMP benchmarks. CPAchecker Workshop, Frauenchiemsee, Germany, 2019.
- G. Ernst. SecCSL: Security Concurrent Separation Logic. Alpine Verification Meeting (AVM), Brno, Czech Republic, 2019.
- G. Ernst. Curious Computation Models. CONNECTIONS Computer Art Workshop by fuzzybinaires, Kreativquartier Munich, Germany, 2019.
- G. Ernst. SecCSL: Security Concurrent Separation Logic. Ringvorlesung of the Software Engineering Graduate Program, Augsburg University, Germany, 2019.
- G. Ernst. Applications of type theory for software verification. TYPES workshop, Munich, Germany, 2019.
- G. Ernst. Hybrid System Falsification by Optimization and Tree Search. Generative Software Development Lab, University of Waterloo, Canada, 2018.
- G. Ernst. Insights and Future Directions from the Verification 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**

- CPAchecker workshop, virtual, 2020.
- CPAchecker workshop, Frauenchiemsee, Germany, 2019.
- Alpine Verification Meeting (AVM), Brno, Czech Republic, 2019.
- CONNECTIONS Computer Art Workshop, Munich, Germany, 2019.
- 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).

### **Testing Competitions**

- Competition on Software Testing (Test-Comp), 2019. Tool: Legion.

## Software Verification Competitions

- VerifyThis Long-term Challenge (2019/2020).
- VerifyThis @ ETAPS, Thessaloniki, Greece, 2018 (co-organizer).
- 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 2018–2020. Tool: FalStar.

## **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)