ECEE Department
University of Colorado Boulder
425 UCB
Boulder, CO 80309
USA
☎ +1 (303) 492 2572
✉ pavol.cerny@colorado.edu
http://ecee.colorado.edu/pavol

Pavol Černý

Curriculum Vitæ (July 29, 2016).

Research Interests

Algorithmic and logical foundations for reliable software. Computer-aided verification. Program synthesis.

Education

2009 **PhD in Computer Science**, *Computer and Information Science Department, University of Pennsylvania, Philadelphia, PA, USA*.

Thesis: Software Model Checking for Confidentiality. Advisor: Rajeev Alur.

2003 **DEA diploma**, *École normale supérieure (ENS), Paris, France*.

Employment

2013 onwards **Assistant Professor**, *Department of Electrical, Computer, and Energy Engineering (ECEE), University of Colorado Boulder, CO, USA*.

2009 - 2012 **Postdoctoral Researcher**, *IST Austria, Klosterneuburg, Austria; Group of Thomas A. Henzinger*.

Summer 2007 **Research Intern**, *Microsoft Research India*.

Summer 2005 **Research Intern**, *NEC Laboratories America*.

Publications

Top 5 publications are in bold.

Selective Conferences

[1] Optimal Consistent Network Updates in Polynomial Time. Pavol Černý, Nate Foster, Nilesh Jagnik, Jedidiah McClurg. In 30th International Symposium on Distributed Computing (DISC), 2016.

[2] Optimizing Horn Solvers for Network Repair. Hossein Hojjat, Philipp Ruemmer, Jedidiah McClurg, Pavol Černý, Nate Foster. In 16th International Conference on Formal Methods in Computer-Aided Design (FMCAD), 2016.

[3] **Event-Driven Network Programming**. Jedidiah McClurg, Hossein Hojjat, Nate Foster, Pavol Černý. In 37th conference on Programming Language Design and Implementation (PLDI), 2016.

[4] Synthesis through Unification. Rajeev Alur, Pavol Černý, Arjun Radhakrishna. In 27th International Conference on Computer Aided Verification (CAV), 2015.

[5] From Non-preemptive to Preemptive Scheduling using Synchronization Synthesis Synthesis through Unification. Pavol Černý, Edmund M. Clarke, Thomas A. Henzinger, Arjun Radhakrishna, Leonid Ryzhyk, Roopsha Samanta, Thorsten Tarrach . In 27th International Conference on Computer Aided Verification (CAV), 2015.

[6] **Efficient Synthesis of Network Updates**. Jedidiah McClurg, Hossein Hojjat, Pavol Černý, Nate Foster. In 36th conference on Programming Language Design and Implementation (PLDI), 2015.

[7] Segment Abstraction for Worst-Case Execution Time Analysis. Pavol Černý, Thomas Henzinger, Laura Kovács, Arjun Radhakrishna, and Jakob Zwirchmayr. In 24th European Symposium on Programming (ESOP), 2015.

[8] Regression-free Synthesis for Concurrency. Pavol Černý, Thomas Henzinger, Arjun Radhakrishna, Leonid Ryzhyk, Thorsten Tarrach. In 26th International Conference on Computer Aided Verification (CAV), 2014.

[9] Efficient Synthesis for Concurrency using Semantics-Preserving Transformations. Pavol Černý, Thomas Henzinger, Arjun Radhakrishna, Leonid Ryzhyk, Thorsten Tarrach. In 25th International Conference on Computer Aided Verification (CAV), 2013.

[10] **Quantitative Abstraction Refinement**. Pavol Černý, Thomas Henzinger, and Arjun Radhakrishna. In 40th Symposium on Principles of Programming Languages (POPL), 2013.

[11] Synthesis from Incompatible Specifications. Pavol Černý, Sivakanth Gopi, Thomas Henzinger, Arjun Radhakrishna, and Nishant Totla. In 12th International Conference on Embedded Software (EMSOFT), 2012.

[12] Interface Simulation Distances. Pavol Černý, Martin Chmelík, Thomas Henzinger, and Arjun Radhakrishna. In 3rd International Symposium on Games, Automata, Logics and Formal Verification (Gandalf), 2012.

[13] Quantitative Synthesis for Concurrent Programs. Pavol Černý, Krishnendu Chatterjee, Thomas Henzinger, Arjun Radhakrishna, Rohit Singh. In 23rd International Conference on Computer Aided Verification (CAV), 2011.

[14] The Complexity of Quantitative Information Flow Problems. Pavol Černý, Krishnendu Chatterjee, Thomas Henzinger. In 24th IEEE Computer Security Foundations Symposium (CSF), 2011.

[15] **Streaming Transducers for Algorithmic Verification of Single-Pass List Processing Programs**. Rajeev Alur and Pavol Černý. In 38th Symposium on Principles of Programming Languages (POPL), 2011.

[16] Simulation Distances. Pavol Černý, Thomas Henzinger, and Arjun Radhakrishna. In 21st International Conference on Concurrency Theory (CONCUR), 2010.

[17] Model Checking of Linearizability of Concurrent Lists. Pavol Černý, Arjun Radhakrishna, Damien Zufferey, Swarat Chaudhuri, and Rajeev Alur. In 22nd International Conference on Computer Aided Verification (CAV), 2010.

[18] Algorithmic Analysis of Array-Accessing Programs. Rajeev Alur, Pavol Černý, and Scott Weinstein. In 18th Conference on Computer Science Logic (CSL), 2009.

[19] Parallel Programming with Object Assemblies. Swarat Chaudhuri, Roberto Lublinerman, and Pavol Černý. In 24th Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA), 2009.

[20] Automated Analysis of Java Methods for Confidentiality. Pavol Černý and Rajeev Alur. In 21st International Conference on Computer Aided Verification (CAV), 2009.

[21] Model Checking on Trees with Path Equivalences. Rajeev Alur, Pavol Černý, and Swarat Chaudhuri. In 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2007. "Best paper coauthored by a student" award.

[22] Preserving Secrecy under Refinement. Rajeev Alur, Pavol Černý, and Steve Zdancewic. In 33rd International Colloquium on Automata, Languages and Programming (ICALP), 2006.

[23] **Synthesis of Interface Specifications for Java Classes**. Rajeev Alur, Pavol Černý, P. Madhusudan, and Wonhong Nam. In 32nd Symposium on Principles of Programming Languages (POPL), 2005.

Refereed Journals

[24] Interface Simulation Distances. Pavol Černý, Martin Chmelík, Thomas Henzinger, and Arjun Radhakrishna. Theoretical Computer Science, 560: 348-363 (2014). Full version of [12].

[25] Algorithmic Analysis of Array-Accessing Programs. Rajeev Alur, Pavol Černý, and Scott Weinstein. ACM Transactions on Computational Logic (TOCL), 13(3) (2012). Full version of [18].

[26] Simulation Distances. Pavol Černý, Thomas Henzinger, and Arjun Radhakrishna. Theoretical Computer Science, 413(1): 21-35 (2012). Full version of [16].

Invited Contributions

[27] From Boolean to Quantitative Synthesis. Pavol Černý and Thomas Henzinger. In 11th International Conference on Embedded Software (EMSOFT), 2011.

[28] Streaming String Transducers. Rajeev Alur and Pavol Černý. In 30th Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2010.

[29] Quantitative Simulation Games. Pavol Černý, Thomas Henzinger, and Arjun Radhakrishna. In Essays in Memory of Amir Pnueli, 2010.

Workshops with proceedings

[30] Performance Search Engine Driven by Prior Knowledge of Optimization. Youngsung Kim, Pavol Černý, John Dennis. In 2nd Workshop on Libraries, Languages and Compilers for Array Programming (ARRAY), 2015.

[31] Toward Synthesis of Network Updates. Andrew Noyes, Todd Warszawski, Pavol Černý, Nate Foster. In 2nd Workshop on Synthesis (SYNT), 2013.

[32] Security Evaluation of ES&S Voting Machines and Election Management System. Adam Aviv, Pavol Černý, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze. In 3rd USENIX/ACCURATE Electronic Voting Technology workshop (EVT), 2008.

Workshops without proceedings

[33] Network Updates for the Impatient: Eliminating Unnecessary Waits. Hossein Hojjat, Jedidiah McClurg, Pavol Černý, Nate Foster. In 1st Workshop on Programming Languages and Verification Technology for Networking (PLVNET), 2015.

[34] Quantitative Simulation Games. Pavol Černý, Thomas Henzinger, and Arjun Radhakrishna. In Games and Probabilistic Models in Formal Verification (GPMFV), 2010.

[35] Assemblies of Objects. Swarat Chaudhuri, Roberto Lublinerman, and Pavol Černý. In 2nd Workshop on Exploiting Concurrency Efficiently and Correctly (EC2), 2009.

Theses

[36] Software Model Checking for Confidentiality. Pavol Černý. PhD thesis. Computer and Information Science department, University of Pennsylvania, Philadelphia, PA, USA. 2009.

[37] Verification by Abstract Interpretation of Parameterized Predicates. Pavol Černý. DEA diploma thesis, École normale supérieure (ENS), Paris, France, 2003.

Report

[38] EVEREST: Evaluation and Validation of Election-Related Standards and Testing. Patrick McDaniel, Matt Blaze, Giovanni Vigna, PIs. A study of electronic voting systems for the State of Ohio. Available on the website of the Ohio Secretary of State. December 2007.

Teaching

University of Colorado Boulder

Fall 2016 ECEN 5033, CSCI 7000-005: Program Synthesis.

Spring 2016 ECEN 4003, CSCI 4830: Concurrent Programming.

Fall 2015 ECEN 5033, CSCI 7000-005: Program Synthesis.

Spring 2015 ECEN 4003, CSCI 4830: Concurrent Programming.

Fall 2014 ECEN 5139, CSCI 5135: Computer-Aided Verification.

Spring 2014 ECEN 5033, CSCI 7000-007: Concurrent Programming.

Fall 2013 ECEN 5139, CSCI 5135: Computer-Aided Verification.

Spring 2013 ECEN 5033, CSCI 7000-007: Program Synthesis.

Previous Courses

Fall 2010 Programming Paradigms for Concurrency. IST Austria and TU Wien, co-instructor.

Spring 2009, Spring 2006 CIS399 C/C++ programming. University of Pennsylvania, co-instructor in Spring 2006, instructor in Spring 2009.

Spring 2009, Fall 2004, Fall 2005 Guest lectures in CIS640 Introduction to Multiprocessor Programming, CSE482 Logic in Computer Science. University of Pennsylvania.

Spring 2005 Teaching Assistant, CIS511 Theory of Computation. University of Pennsylvania.

Fall 2004 Teaching Assistant, CSE482 Logic in Computer Science. University of Pennsylvania.

Students

Since Fall 2013 Jedidiah McClurg (PhD).

Since Fall 2016 Nick Lewchenko (PhD).

Since Fall 2015 Tianhan Lu (PhD). Co-advised with Evan Chang.

Since Fall 2015 Saeid Tizpaz Niari (PhD).

Alumni

- Nilesh Jagnik. MS Spring 2016. Optimal Consistent Network Updates in Polynomial Time [1]. First employment: Google.
- Parker Evans. (Undergraduate) Discovery Learning Apprenticeship, 2013-14.
- Prabhash Krishnan (2015-16), Aniket Lata (2015-16), Krishna Sripada (2015-16), Vaibhav Singh (2014-15). (Graduate) Independent Study.

Co-supervised Students at IST Austria

2009-14 Worked closely with Arjun Radhakrishna on model checking and synthesis for concurrent programs [17],[13],[9],[8] and on quantitative verification and synthesis [16],[26],[29],[12],[11],[10],[24],[7]. A.R. was a doctoral student of Thomas Henzinger.

Fall 2012 Co-supervised Thorsten Tarrach's rotation on Efficient Synthesis for Concurrency using Semantics-Preserving Transformations [9].

Spring 2012 Co-supervised Martin Chmelík's rotation on Interface Simulation Distances [12],[24].

Summer 2011 Co-supervised Nishant Totla's and Sivakanth Gopi's internship on Synthesis from Incompatible Specifications [11].

Summer 2010 Co-supervised Rohit Singh's internship on Quantitative Synthesis for Concurrent Programs [13].

Awards

- Microsoft Research Cambridge award for best paper co-authored by a student at TACAS 2007.
- Bourse du Gouvernement Français (French Government Stipend), 2000-2003.
- Winner (one of six) of Olympiad in Computer Science, national round, Slovakia, 1998.

Selected Research Projects

2015–present **Event-Driven Network Programming.** Theory and algorithms for event-driven network programming. Work described in [3].

2013–2015 **Synthesis for Network Updates.** A framework, algorithms, and tools for synthesis of safe updates of global network policies. Work described in [1],[2],[6],[33],[31].

2013–present **Synthesis for Concurrent Programs.** Algorithms for efficient synthesis of concurrent programs, with applications to device drivers. Work described in [9],[8],[5],[4].

2010–present **Quantitative Verification and Synthesis.** Algorithms and tools for verification and synthesis that take into account quantitative measures such as performance, fault tolerance, information flow, and resource consumption. Work described in [16],[26],[13],[14],[27],[29],[12],[11],[10],[24],[30],[7].

2010–2011 **Streaming Transducers for Program Verification.** A new, expressively robust, and analyzable transducer model with applications in verification of list-processing and string-processing programs. Work described in [15],[28].

2009 **Model Checking for Concurrent Data Structures.** Introduced techniques for model checking for concurrent data structures and developed CoLT, a tool for verifying their Java implementations. Work described in [17]. Project website: `http://www.ist.ac.at/~cernyp/colt`.

2008–2009 **Programming Abstractions for Data Parallel Programs.** A data-centric programming model called Chorus and a language and runtime system called JChorus for irregular data parallel applications based on the idea of spatial locality. Work described in [19].

2005–2009 **Software Model Checking for Confidentiality.** A specification framework for confidentiality, novel decision procedures for finite state systems and for classes of programs, and abstraction-based program analysis techniques. Implemented a tool ConAn (for CONfidentiality ANalysis) for checking confidentiality properties of midlets for mobile devices. Work described in [36],[18],[20],[21],[22].

2007 **Security Evaluation of ES&S Voting Machines and Election Management System.** Member of a team conducting security evaluation of voting machines and software in the project EVEREST, commissioned by the Ohio Secretary of State. I led the efforts in static analysis of the backend system. Work described in [38],[32].

2007 **Integrity Analysis for Windows Vista.** Methods for analysis of possible vulnerabilities in Vista access control system, which is based on integrity levels that can change over time. Supervisors: Sriram Rajamani, Prasad Naldurg. Microsoft Research India, May-August, 2007.

2003–2005 **JIST project.** Automatic synthesis of behavioral interfaces for Java classes using predicate abstraction, learning algorithm L* and symbolic model checking. Work described in [23].

2003 **Verification by Abstract Interpretation of Parameterized Predicates.** DEA diploma thesis, 2003. Generalizes predicate abstraction in order to reason about programs on arrays (e.g. sorting programs). Supervisor: Patrick Cousot. ENS, Paris, France. Work described in [37].

Selected Talks

Invited Talks

- Synthesizing Event-driven Network Programs from Scenarios. 5^{th} Workshop on Synthesis (SYNT), Toronto, Canada, 2016.
- Program Synthesis for Network Updates. 1^{st} NetPL workshop on programming languages for networks, Prague, Czech Republic, 2015
- Program Synthesis for Network Updates. 7^{th} Interaction and Concurrency Experience (ICE) workshop, Berlin, Germany, 2014
- Quantitative Abstraction Refinement. Rich Model Toolkit COST Action meeting, co-located with HVC 2012, Haifa, Israel, 2012.
- Quantitative Synthesis for Concurrent Programs. 4^{th} Workshop on Games for Design, Verification and Synthesis (GASICS), Newcastle, UK, 2012.

Seminar Talks

- Event-Driven Network Programming. IST Austria, 2016.
- Trace-based Synchronization Synthesis for Device Drivers. Intel Research, Hillsboro, OR, USA, 2016.
- From Non-preemptive to Preemptive Scheduling using Synchronization Synthesis. Intel Research, Hillsboro, OR, USA, 2015.
- Program Synthesis for Concurrency. Xilinx, Longmont, CO, USA 2014.
- Program Synthesis for Network Updates. Kempner Colloquium, joint Mathematics and Applied Mathematics departments colloquium, University of Colorado Boulder, 2014; CISL seminar, NCAR, Boulder, CO, USA 2014; Dagstuhl seminar 15071 on Formal Foundations on Networking, 2015; IST Austria, 2014.
- Regression-free Synthesis for Concurrency. Intel Research, Hillsboro, OR, USA, 2014.
- Toward Synthesis of Network Updates. IST Austria, 2013.
- Efficient Synthesis for Concurrency using Semantics-Preserving Transformations. Intel Research, Hillsboro, OR, USA, 2013.
- Quantitative Abstraction Refinement. Verimag, Grenoble, France, 2012. ERC meeting, Brussels, Belgium, 2012. Tel Aviv University, Tel Aviv, Israel, 2012.
- From Boolean to Quantitative Synthesis. University of Colorado, Boulder, CO, USA, 2012.
- Inductive Synthesis for Automata Education. Microsoft Research, Redmond, WA, USA, 2012.
- Quantitative Synthesis for Concurrent Programs. ERC meeting, Venice, Italy, 2011. Intel Research, Hillsboro, OR, USA, 2012.

- Algorithmic Software Verification for Data Structures. EPFL, Switzerland; Rice University, TX, USA; Leicester University, UK; Queen Mary, University of London, UK; University of Birmingham, UK; 2011.
- Streaming Transducers for Algorithmic Verification of Single-Pass List Processing Programs. Alpine Verification Meeting, Lausanne, Switzerland, 2010. RiSE seminar, TU Wien, Austria, 2010; Masaryk University, Brno, Czech Republic, 2011; Charles University, Prague, Czech Republic, 2011.
- Model Checking of Linearizability of Concurrent Data Structures. Univerite Paris VII, Paris, France; Graz University of Technology, Graz, Austria, 2010.
- Software Model Checking for Confidentiality. NASA Ames Research Center, CA, USA; INRIA Rennes, France; EPFL, Switzerland; Pennsylvania State University, PA, USA, 2009.
- A Unified Framework for Integrity Analysis in Windows Vista. Microsoft Research India, 2007.
- Algorithmic Verification of Secrecy. IBM Research, 2007.
- Model Checking on Trees with Path Equivalences. Penn Security Seminar.
- Preserving Secrecy under Refinement. Penn Programming Languages Club.
- Pointer analysis in FSoft. NEC Labs America, 2005.
- Verification by Abstract Interpretation of Parameterized Predicates. SAI seminar, ENS, Paris, France. 2003.
- Static Analyses for Efficient Execution of PVS. SRI, 2002.

Professional Service

- Program committee co-chair of EC2 2016, PLVNET 2015, SYNT 2015.
- Program committee member for CAV 2016, TACAS 2016, GandALF 2015, EC2 2015, CAV 2014, EMSOFT 2014, SYNT 2014, MEMICS 2011.
- External review committee (ERC) member for POPL 2016.
- Sponsorship chair for CAV 2016.
- Graduate Committee, ECEE, 2013-present.
- PhD Thesis Committee for Zyad Hassan (ECEE, CU Boulder, 2014), Saqib Sohail (ECEE, CU Boulder, 2014), Arjun Radhakrishna (IST Austria, 2014), Thomas Nelson (ECEE, CU Boulder, 2015), Samuel Blackshear (CS, CU Boulder, 2015), Aleksandar Chakarov (proposal, CS, CU Boulder, 2015), Thorsten Tarrach (IST Austria, 2016), Hadi Ravanbakhsh (proposal, ECEE, CU Boulder, 2016).
- PhD Preliminary Examination committee for Michael Dooley (ECEE, CU Boulder), Aleksandar Chakarov (CS, CU Boulder), Thorsten Tarrach (IST Austria), Michael Coughlin (ECEE, CU Boulder), Hadi Ravanbakhsh (ECEE, CU Boulder), Jedidiah McClurg (CS, CU Boulder, advisor).
- MS Thesis committee for Ali Ismail (ECEE, CU Boulder, 2015), Suhas Kumar (ECEE, CU Boulder, 2016), Nilesh Jagnik (CS, CU Boulder, 2016, advisor).
- Senior Thesis committee for Ross Holland (CS, CU Boulder), Nick Vanderweit (CS, CU Boulder), Evan Roncevich (CS, CU Boulder).
- Reviewer for conferences and workshops: POPL, CAV, LICS, PLDI, ESOP, ICALP, CSL, FOSSACS, FMCAD, APLAS, Usenix Security, TACAS, PLAN-X, Gandalf, MFCS, LPAR, CSF, FM, SAS.

- Reviewer for journals: Theoretical Computer Science, Communications of the ACM, Journal of Computer Security, IET Software journal, ACM Transactions on Embedded Computing Systems, IEEE Transactions on Software Engineering, Formal Methods in System Design, Acta Informatica.
- Reviewer for Handbook of Model Checking *(to appear)*.
- Panelist for National Science Foundation (US).
- Reviewer for the Czech Science Foundation (Czech Republic).
- Joint IST Austria / TU Wien verification seminar, February 2010 - January 2011, organizer.
- NEVER 4-ever, 4th Northeastern Verification Workshop, 2007, Co-organizer.
- Research Forum at Penn Engineering 2007, Graduate Student Planning Committee member.

Software

- Liss. A tool for synchronization synthesis for concurrent programs [5]. Available at: `https://github.com/thorstent/Liss` .
- CoLT (Concurrency using Lockstep Tool). A tool for model checking of linearizability of concurrent data structures [17]. Tool web page: `http://www.ist.ac.at/~cernyp/colt` .
- Chorus. A compiler and runtime for a programming model for data parallel programs [19].
- ConAn (CONfidentiality ANalysis). Verification of confidentiality properties of Java midlets for mobile devices [20].
- Jist (Java Interface Synthesis Tool). A tool for synthesis of behavioral interfaces for Java classes [23].

Funding

- Travel and Registration Support for Computer Aided Verification 2016, PI. NSF. $15K. Supports student participation at CAV 2016.
- Auditr: Securing Space/Time Defenses in Java Bytecode. 2015-2019, PI. CU Boulder co-PIs: John Black, Bor-Yuh Evan Chang, Sriram Sankaranarayanan. Subcontracts: UT Austin (Isil Dillig (PI), Marijn Heule (co-PI)); Kestrel Technology (Henny Sipma (PI)). DARPA, STAC program. $5.7M ($2.8M for CU Boulder).
- Mining and Understanding Bug Fixes to Address Application-Framework Protocol Defects. 2014-2018, co-PI. PI: Bor-Yuh Evan Chang; other co-PIs: Kenneth Anderson, Sriram Sankaranarayanan, Tom Yeh. DARPA, MUSE program. $1.6M.
- Practical Synthesis of Network Updates. 2014-2017, PI. Other PI: Nate Foster, Cornell. NSF. $246K for CU Boulder.
- Automatic Synthesis of High-Assurance Device Drivers. PI. Other PIs: Leonid Ryzhyk, Michael Stumm (University of Toronto), Gernot Heiser (NICTA), Alastair Donaldson (Imperial College London). Awarded, 2013. Gift from Intel Corporation to CU Boulder: $300.000.
- Automated tutor for automata education, $10,000. Co-author. PI: T. Henzinger. Grant from Microsoft Research, Awarded, December 2010.
- RiSE. Co-author. PIs: Thomas Henzinger and others. Austrian National Research Network on Rigorous Software Engineering. Awarded, 2010.
- Travel grants from Usenix Security Conference, 2008 and from Marktoberdorf Summer School, 2006.

Miscellaneous

- Citizenship: Slovak Republic.
- ".v sieti" column on everything Web related for the Slovak magazine Tyzden, 2004-2006.