Nicolás Rosner

2024 Anacapa St., Santa Barbara, CA 93105
rosner@cs.ucsb.edu, nrosner@gmail.com
https://nicorosner.com   (805) 724-9174

Researcher in computer science with 10+ years of experience in formal methods, verification, and security. Strong combination of theoretical research, hands-on engineering, and leadership experience.

RESEARCH INTERESTS

Formal methods. Software engineering. Cybersecurity.
Automated software verification. Constraint solving. Symbolic execution. Distributed systems.
Automated vulnerability detection. Side-channel analysis. Network information leakage.

EDUCATION

PhD in Computer Science, University of Buenos Aires (UBA), 2015.
Dissertation: Distributed techniques for efficient bounded verification.
Advisor: Marcelo Frias. Committee: Sebastian Elbaum, Bernd Fischer, Sebastian Uchitel.

MS in Computer Science, UBA, 2006.
Thesis: ParAlloy, a distributed implementation of DynAlloy.
Advisors: Marcelo Frias, Carlos López Pombo.

RESEARCH EXPERIENCE

Postdoctoral Researcher, University of California Santa Barbara (UCSB), 2016–present.
Verification Lab (PI Tevfik Bultan).
DARPA STAC (Space/Time Analysis for Cybersecurity) program.
Information leakage quantification for encrypted network communications.
Synthesis of adaptive side-channel attacks in noisy network environments.
Represented the Verification Lab 3 times in DARPA competitions, with outstanding results.
Guidance and mentoring of PhD students.

Assistant Professor, Buenos Aires Institute of Technology (ITBA), 2015–2016.
CISoft Reliable Software Lab (PI Marcelo Frias).
Automated verification and testing of code involving nonprimitive data types.
Symbolic execution with lazy initialization for heap-allocated data structures.
Mentored PhD students. Supervised student research projects.

Full-Time Researcher, UBA, 2011–2015.
Research Assistant, UBA, 2007–2011.
Relational Formal Methods Lab (PI Marcelo Frias).
Distributed verification of Java code annotated with JML contracts.
Parallel analysis of Alloy models. Techniques based on constraint solving.
Supervised two MS theses. Mentored dozens of undergraduate students.

PUBLICATIONS

N. Rosner, B. Kadron, L. Bang, T. Bultan. Profit: Detecting and Quantifying Side Channels in Networked Applications. Network and Distributed System Security Symposium (**NDSS 2019**).

I. Bocić, T. Bultan, **N. Rosner**. Inductive Verification of Data Model Invariants in Web Applications Using First-Order Logic. Automated Software Engineering (**ASE Journal 2019**).

L. Bang, **N. Rosner**, T. Bultan. Online Synthesis of Adaptive Side-Channel Attacks Based on Noisy Observations. IEEE European Symposium on Security and Privacy (**Euro S&P 2018**).

T. Brennan, N. Tsiskaridze, **N. Rosner**, A. Aydin, T. Bultan. Constraint normalization and parameterized caching for quantitative program analysis. ACM Symposium on Foundations of Software Engineering (**FSE 2017**).

N. Rosner, J. Geldenhuys, N. Aguirre, W. Visser, M. Frias. BLISS: Improved Symbolic Execution by Bounded Lazy Initialization with SAT Support. IEEE Transactions on Software Engineering (**TSE 2015**).

N. Rosner, V. Bengolea, P. Ponzio, S. Khalek, N. Aguirre, M. Frias, S. Khurshid. Bounded Exhaustive Test Input Generation from Hybrid Invariants. ACM Conference on Object-Oriented Programming, Systems, Languages and Applications (**OOPSLA 2014**).

P. Ponzio, **N. Rosner**, N. Aguirre, M. Frias. Efficient Tight Field Bounds Computation Based on Shape Predicates. International Symposium on Formal Methods (**FM 2014**).

J. Galeotti, **N. Rosner**, C. Pombo, M. Frias. TACO: Efficient SAT-Based Bounded Verification Using Symmetry Breaking and Tight Bounds. IEEE Transactions on Software Engineering (**TSE 2013**).

N. Rosner, J. Siddiqui, N. Aguirre, S. Khurshid, M. Frias. Ranger: Parallel Analysis of Alloy Models by Range Partitioning. IEEE/ACM Conference on Automated Software Engineering (**ASE 2013**).

N. Rosner, J. P. Galeotti, S. Bermudez, G. Marucci, S. Pérez, L. Pizzagalli, L. Zemin, M. Frias. Parallel Bounded Analysis of Code with Rich Invariants by Refinement of Field Bounds. International Symposium on Software Testing and Analysis (**ISSTA 2013**).

N. Rosner, C. Pombo, N. Aguirre, A. Jaoua, A. Mili, M. Frias. Parallel Verification of Alloy Models by Transcoping. Verified Software: Theories, Tools, and Experiments (**VSTTE 2013**).

J. Galeotti, **N. Rosner**, C. Pombo, M. Frias. Analysis of Invariants for Efficient Bounded Verification. International Symposium on Software Testing and Analysis (**ISSTA 2010**).

N. Rosner, J. Galeotti, C. Pombo, M. Frias. ParAlloy: Towards a Framework for Efficient Parallel Analysis of Alloy Models. Abstract State Machines, Alloy, B and Z (**ASM 2010**).

J. Galeotti, **N. Rosner**, C. Pombo, M. Frias. Distributed SAT-based Analysis of Object-Oriented Code. International Symposium on Automatic Program Verification (**APV 2009**).

RESEARCH TOOL DEVELOPMENT

Profit	Side-channel analysis of networked applications	Author
Cashew	Constraint normalization and caching for SMT model counters	Co-author
ABC	Automata-based model-counting constraint solver	Contributor
Ranger	Distributed analysis of Alloy models by range partitioning	Author
HyTek	Test generation for complex types using hybrid input specifications	Author
TACO	Verification of Java code annotated with JML contracts	Co-author
MUCHO-TACO	Distributed version of TACO based on bounds refinement	Author
AlloyCLI	Experimental batch version of Alloy Analyzer	Author
ParAlloy	Distributed version of DynAlloy based on decomposition	Author
DynAlloy	Extension of Alloy with actions	Contributor

TALKS

Detecting and Quantifying Side Channels in Networked Applications.
Network and Distributed System Security Symposium (**NDSS 2019**).

Speeding Up Symbolic Execution using Tight Field Bounds (2016 talk series).
CS Department, Georgia Tech
CS Department, University of Minnesota
CS Department, University of California Santa Barbara
National Institute of Aerospace, Langley, VA.

Bounded Exhaustive Test Input Generation from Hybrid Invariants.
Int'l Conference on Object-Oriented Programming, Systems, Languages and Applications (**OOPSLA 2014**).

Distributed Approaches for Software Verification Engines.
Argentinian Workshop on Foundations for Automatic Software Analysis and Construction (**FACAS 2014**).

Parallel Analysis of Alloy Models by Range Partitioning.
Argentinian Symposium on Software Engineering (**ASSE 2014**).

Parallel Analysis of Alloy Models by Range Partitioning.
IEEE/ACM International Conference on Automated Software Engineering (**ASE 2013**).

Parallel Bounded Analysis of Code with Rich Invariants by Refinement of Field Bounds.
International Symposium on Software Testing and Analysis (**ISSTA 2013**).

BLISS: Bounded Lazy Initialization with SAT-Solver Support.
Workshop on Formal Methods, International Conference on Concurrency Theory (**CONCUR 2013**).

Distributed Verification of Alloy Models.
Argentinian Workshop of Foundations for Automatic Software Analysis and Construction (**FACAS 2013**).

Distributed SAT-based Analysis of Object-Oriented Code (with J. P. Galeotti).
International Symposium on Automatic Program Verification (**APV 2009**).

GRANTS

Supervised by PI Marcelo Frias.
Participated as researcher and collaborated in proposal writing for the following grants:

Efficient Automated Software Analysis based on Constraint Solving, 2014–2017. (PICT 2014 #2624).
Funded by the National Agency for Science and Technology, Argentina. AR$ 424,000.

Scalable Analysis of Models and Applications Based on SAT-Solving, 2011–2014. (PICT 2011 #1689).
Funded by the National Agency for Science and Technology, Argentina. AR$ 250,000.

Scalable Software Analysis Using Techniques Based on Constraint Solving, 2008–2011. (PICT 2008 #2484).
Funded by the National Agency for Science and Technology, Argentina. AR$ 256,000.

Software Analysis and Verification Based on SAT-Solving Techniques, 2008–2011. (UBACyT #X082).
Funded by the University of Buenos Aires, Argentina. AR$ 35,000.

TEACHING EXPERIENCE

Assistant Professor, ITBA, 2015–2016.
Taught graduate and undergraduate courses. Mentored PhD and MS students.

Course Supervisor, UBA, 2013–2015.
In charge of an undergraduate course each semester, some with 100+ students.
Created course-wide standards and processes for lecturing and evaluation.
Designed lab projects and midterms. Directly supervised up to 8 TAs per semester.
Helped TAs develop their lecturing, public speaking, and question-answering skills.

Lead Teaching Assistant, UBA, 2007–2013.
Led discussion sections. Graded lab projects and midterms.
Collaborated in the design of lab projects. Mentored junior TAs.

Teaching Assistant, UBA, 2003–2007.
Participated in discussion sections. Graded lab projects and midterms.

Courses taught
Algorithms and Data Structures
Advanced Algorithms and Data Structures
Operating Systems
Programming Language Paradigms
Automated Software Verification and Testing
Functional Programming

GRADUATE STUDENT SUPERVISION

Matías H. Pérez, MS 2016.
Thesis: Learning and restarts in a distributed SAT-solver.

Ignacio Vissani, MS 2013.
Thesis: Inheritance of learned clauses in parallel satisfiability solving.

GRADUATE COMMITTEE MEMBERSHIP

Virginia Brassesco, MS 2017.
Thesis: Concurrent controller synthesis for GR(1)-goal-defined games.

Martin Epszteyn, MS 2014.
Thesis: Efficient computing of absolutely normal numbers.

Ezequiel Castellano, MS 2014.
Thesis: Synthetic techniques to improve latency in discrete controllers.

PROFESSIONAL SERVICE

International Symposium on Software Testing and Analysis

Artifact Evaluation Co-Chair	**ISSTA 2018**
Publicity Chair	**ISSTA 2018**
Publicity Chair	**ISSTA 2017**

International Conference on Software Engineering

Program Committee Member, Demos Track	**ICSE 2017**
Student Volunteer Co-Chair	**ICSE 2017**

European Conference on Object-Oriented Programming

Publicity Chair	**ECOOP 2018**

ICSE Workshop on Software Engineering Education for Millennials

Program Committee Member	**SEEM 2018**

ICSE Workshop on Software Engineering Curricula for Millennials

Program Committee Member	**SECM 2017**

Argentinian Workshop on Foundations for Automatic Software Analysis and Construction

General Chair	**FACAS 2016**

SCHOLARSHIPS

Full-time scholarship for PhD program at the University of Buenos Aires.
Funded by the National Scientific Research Council of Argentina.

OUTREACH AND UNIVERSITY SERVICE

At the Department of Computer Science, UBA.

Departmental Council Member, 2014–2015.

Departmental Chair of Outreach and Popularization of Science, 2014–2015.
Designed activities to promote CS among high school students.
Targeted vulnerable school districts of Buenos Aires underrepresented at UBA.
Coordinated efforts with public and private institutions. Secured grants to support activities.
Chaired the organization of **Computer Science Week**, a yearly event with 1,500 students from 40 schools.
Led the Department's **Robotics in Schools** program, which won a Google CS4HS grant.
Led the Department's **Student Ambassadors** program.

MAIN PROGRAMMING LANGUAGES

Python, Java, C++, Mathematica, bash-fu.

SPOKEN LANGUAGES

Fluent in English, Spanish, French, and German.

REFERENCES

Tevfik Bultan	bultan@cs.ucsb.edu	University of California Santa Barbara
Marcelo Frias	mfrias@itba.edu.ar	Buenos Aires Institute of Technology
Sebastian Uchitel	suchitel@dc.uba.ar	University of Buenos Aires
Sarfraz Khurshid	khurshid@ece.utexas.edu	University of Texas at Austin
Corina Pasareanu	corina.pasareanu@west.cmu.edu	CMU West & NASA Ames
Willem Visser	wvisser@cs.sun.ac.za	Stellenbosch University