

Curriculum Vitae

Personal information

Name: Cătălin Hrițcu
Birthdate: 30th of July, 1982
Citizenship: Romanian
E-mail: catalin.hritcu@gmail.com
Address: University of Pennsylvania, CIS dept.
3330 Walnut Street, Philadelphia, PA 19104-6389, U.S.A.
Homepage: <http://purl.org/hritcu/homepage>

Currently

May 2011 – now Research Associate at University of Pennsylvania; DARPA CRASH/SAFE project
Advisor: Prof. Benjamin C. Pierce
July 2007 – now Ph.D. Student at Saarland University, Information Security and Cryptography Group
Advisors: Michael Backes, Matteo Maffei, Andrew D. Gordon (MSR)

Research Interests

Language-based Security secure protocol implementation, protocol analysis, symbolic abstractions of cryptography, electronic voting

Type Systems refinement types, union and intersection types, semantic subtyping

Semantics of Programming Languages step-indexed models, higher-order store, concurrency, formalized metatheory

Verification abstract interpretation, software model checking, program logics

Formal Methods in Software Engineering tools for improving the security of production code, automatic code generation, certified tools

Academic Degrees

May 2007 Master of Science in Computer Science, Honors degree
(GPA: 1.0/1.0), Saarland University, Saarbrücken, Germany
June 2005 Licentiate Degree (4 years) in Computer Science, Honors degree
(GPA: 9.9/10.0), “Al. I. Cuza” University of Iași, Romania

Award

February 2008 Günter Hotz Medal for outstanding CS graduates, Saarland University

Fellowships and Scholarships

Jun.'08 – Apr.'11 Ph.D. fellowship from Microsoft Research Cambridge (UK) and the IMPRS-CS
Oct.'05 – May'08 M.Sc. and then Ph.D. fellowship from the International Max Planck Research School for Computer Science (IMPRS-CS)
Apr.'04 – Sept.'04 Socrates-Erasmus scholarship at Technical University Braunschweig
2001 – 2005 Scholarship for high academic achievements from Romanian government

Internships

Sept.–Nov. 2009 Microsoft Research Cambridge (UK), Semantic Subtyping with an SMT Solver
Summers '05, '06, '07 Google “Summer of Code” participant with XWiki.org

Selected Publications

- Journals Gavin M. Bierman, Andrew D. Gordon, Cătălin Hrițcu, and David Langworthy. Semantic subtyping with an SMT solver. To appear in *Journal of Functional Programming*, Cambridge University Press, December 2011.
- Cătălin Hrițcu and Jan Schwinghammer. A step-indexed semantics of imperative objects. *Logical Methods in Computer Science (LMCS)*, 5(4:2):1–48, December 2009.
- Conferences Michael Backes, Cătălin Hrițcu, and Thorsten Tarrach. Automatically verifying typing constraints for a data processing language. In *First International Conference on Certified Programs and Proofs (CPP 2011)*, pages 296–313. Springer, December 2011.
- Michael Backes, Cătălin Hrițcu, and Matteo Maffei. Union and intersection types for secure protocol implementations. In *Theory of Security and Applications (TOSCA 2011)*. Invited paper, April 2011, to appear.
- Gavin M. Bierman, Andrew D. Gordon, Cătălin Hrițcu, and David Langworthy. Semantic subtyping with an SMT solver. In *15th ACM SIGPLAN International Conference on Functional programming (ICFP 2010)*, pages 105–116. ACM Press, September 2010.
- Michael Backes, Martin P. Grochulla, Cătălin Hrițcu, and Matteo Maffei. Achieving security despite compromise using zero-knowledge. In *22th IEEE Symposium on Computer Security Foundations (CSF 2009)*, pages 308–323. IEEE Computer Society Press, July 2009.
- Michael Backes, Cătălin Hrițcu, and Matteo Maffei. Type-checking zero-knowledge. In *15th ACM Conference on Computer and Communications Security (CCS 2008)*, pages 357–370. ACM Press, October 2008.
- Michael Backes, Cătălin Hrițcu, and Matteo Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In *21th IEEE Symposium on Computer Security Foundations (CSF 2008)*, pages 195–209. IEEE Computer Society Press, June 2008.
- Thesis Cătălin Hrițcu. *Union, Intersection, and Refinement Types and Reasoning About Type Disjointness for Security Protocol Analysis*. PhD thesis, Information Security and Cryptography Group, Saarland University, November 2011. Manuscript.

Advised Students

- April 2011 **Alex Busenius**. *Mechanized Formalization of a Transformation from an Extensible Spi Calculus to Java*. (Master’s Thesis)
- August 2010 **Thorsten Tarrach**. *Automatically Verifying “M” Modeling Language Constraints*. (Master’s Thesis)
- January 2009 **Martin Grochulla**. *Security Despite System Compromise with Zero-Knowledge Proofs*. (Master’s Thesis; co-advised with Matteo Maffei)
- October 2008 **Alex Busenius**. *Expi2Java – An Extensible Code Generator for Security Protocols*. (Bachelor’s Thesis)

October 2008 **Thorsten Tarrach.** *Spi2F# – A Prototype Code Generator for Security Protocols.*
(Bachelor’s Thesis)

Teaching Assistant

Summer 2009 *Practical Aspects of Security (best lecture award)*
Advanced Lecture, Saarland University, Instructor: Prof. Dr. Michael Backes

Winter 2008/09 Seminar, Saarland University, Instructor: Prof. Dr. Michael Backes
Topic: *Observational Equivalence for Security Protocols*

Winter 2007/08 Seminar, Saarland University, Instructor: Prof. Dr. Michael Backes
Topic 1: *The Analysis of Electronic Voting Protocols*
Topic 2: *The Secure Implementation of Cryptographic Protocols*

Summer 2007 *Introduction to Computational Logic*
Core Lecture, Saarland University, Instructor: Prof. Dr. Gert Smolka

Winter 2006/07 *Language-based Security*
Advanced Lecture, Saarland University, Instructor: Dr. Matteo Maffei

Recent Software Projects

2010 **DVerify** a verification condition generator for Microsoft’s codename “M” language
(by Thorsten Tarrach, coordinated only)

2009 – 2010 **Dminor** a type-checker for “M” using semantic subtyping and an SMT solver
(with Andy Gordon, Gavin Bierman, and David Langworthy)

2009 – now **F5** a type-checker and toolchain for an extension of Refined Concurrent FPC (RCF)
with union, intersection and polymorphic types (with Thorsten Tarrach)

2008 – 2011 **Expi2Java** code generator that converts verifiable protocol models into interoperable
Java implementations (by Alex Busenius, coordinated only)

2008 – now **zk-typechecker** the first type-checker for automatically analyzing protocols that
use zero-knowledge proofs (with Stefan Lorenz, Kim Pecina and Thorsten Tarrach)

References

Benjamin C. Pierce

Professor, CIS Department, University of Pennsylvania
3330 Walnut Street, Philadelphia, PA 19104-6389; Phone: +1 215 898-6222
E-mail: bcpierce@cis.upenn.edu

Michael Backes

Professor, Head of the Information Security and Cryptography Group,
Saarland University and MPI-SWS
Postfach 15 11 50, 66041-D Saarbrücken, Germany; Phone: +49 681 302 3259
E-mail: backes@mpi-sws.mpg.de

Matteo Maffei

Leader of Junior Research Group for Language-based Security, Saarland University
Postfach 15 11 50, 66041-D Saarbrücken, Germany; Phone: +49 681 302 57368
E-mail: maffei@cs.uni-sb.de

Andrew D. Gordon

Principal Researcher, Microsoft Research Cambridge
Professor at the School of Informatics of University of Edinburgh
Roger Needham Building, 7 J J Thomson Ave, Cambridge CB3 0FB, UK;
Phone: +44 1223 479780
E-mail: adg@microsoft.com

Gert Smolka

Professor, Head of the Programming Systems Lab, Saarland University
Postfach 15 11 50, 66041-D Saarbrücken, Germany; Phone: +49 681 302 5311
E-mail: smolka@ps.uni-sb.de

December 11, 2011