Cătălin Hriţcu

Curriculum Vitae

Contact

Inria Prosecco, 2 rue Simone Iff, 75012 Paris, France

catalin.hritcu@gmail.com http://prosecco.gforge.inria.fr/personal/hritcu/

Education

06/2007–01/2012 **Ph.D.** in Computer Science from Saarland University, **Summa cum Laude**, Advisors: Michael Backes (official supervisor), Matteo Maffei, and Andrew D. Gordon

10/2005–05/2007 **M.Sc.** in Computer Science from Saarland University, Saarbrücken, Germany, **Honors degree**, Thesis advisors: Gert Smolka and Jan Schwinghammer

09/2001–06/2005 **Licentiate** (4 years undergrad degree) in Computer Science from "Alexandru Ioan Cuza" University, Iaşi, Romania, **Honors degree**

Positions

10/2013–now **Research Scientist** (chargé de recherche; tenured) at Inria Paris in the Prosecco team

05/2011–09/2013 **Research Associate** at University of Pennsylvania; DARPA CRASH/SAFE project; Supervisor: Benjamin C. Pierce

Grants

10/2015–10/2018 **Ph.D. grant** co-financed by the French Department of Defense (DGA) and Inria on "Micro-Policies: High-Assurance Hardware-Assisted Security Monitors"

starting in 2016 **Ph.D. grant** financed by Microsoft Research PhD Scholarship Programme on "F⋆: From Program Verification System to Proof Assistant"

Awards

03/2016 **Inria Award for PhD Supervising and for Research** (PEDR)

02/2008 **Günter Hotz Medal** for outstanding CS graduates, Saarland University

Fellowships

03/2007–04/2011 **Ph.D. fellowship** from Microsoft Research Cambridge (UK) and the IMPRS-CS

10/2005–02/2007 **M.Sc. fellowship** from the International Max Planck Research School for Computer Science (IMPRS-CS)

Internship

09/2009–11/2009 Microsoft Research Cambridge (UK), Semantic Subtyping with an SMT Solver

Advised Students

10/2015–now **PhD supervisor** of Yannis Juglaret (Université Paris Diderot – Paris 7); works on Micro-Policies; funded by grant co-financed by DGA and Inria

08/2011–now **External PhD co-supervisor** of Arthur Azevedo de Amorim (University of Pennsylvania, official supervisor: Benjamin C. Pierce)

01/2016–now **Currently supervising 3 MSc internships**: Guido Martínez (National University of Rosario), Diane Gallois-Wong (ENS Paris), Alejandro Aguirre (Paris 7)

10/2008–12/2015 **Previously supervised 8 MSc internships/theses**, all of which have resulted in research papers (6 of them published at good conferences and 2 in preparation). 5 of the 8 advised MSc students are following a PhD (1 at Inria, 2 at Princeton, 1 at IST Vienna, and 1 at MPI-INF Saarbrücken).

Publications

Journals

[1] Arthur Azevedo de Amorim, Nathan Collins, André DeHon, Delphine Demange, Cătălin Hriţcu, David Pichardie, Benjamin C. Pierce, Randy Pollack, and Andrew Tolmach. A verified information-flow architecture. arXiv:1509.06503; Accepted in Special Issue of the Journal of Computer Security (JCS) on Verified Information Flow Security. To appear, September 2015.

[2] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Union, intersection, and refinement types and reasoning about type disjointness for secure protocol implementations. *Journal of Computer Security (JCS); Special Issue on Foundational Aspects of Security*, 22(2):301–353, February 2014.

[3] Gavin M. Bierman, Andrew D. Gordon, Cătălin Hriţcu, and David Langworthy. Semantic subtyping with an SMT solver. *Journal of Functional Programming (JFP)*, 22(1):31–105, March 2012.

[4] Cătălin Hriţcu and Jan Schwinghammer. A step-indexed semantics of imperative objects. *Logical Methods in Computer Science (LMCS)*, 5(4:2):1–48, December 2009.

Book

[5] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. *Software Foundations*. Electronic textbook, Version 4.0 beta, January 2016.

Conferences

[6] Nikhil Swamy, Cătălin Hriţcu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cédric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, Jean-Karim Zinzindohoue, and Santiago Zanella-Béguelin. Dependent types and multi-monadic effects in F*. In *43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 256–270. ACM, January 2016. (Acceptance rate: 59/253=0.23).

[7] Zoe Paraskevopoulou, Cătălin Hriţcu, Maxime Dénès, Leonidas Lampropoulos, and Benjamin C. Pierce. Foundational property-based testing. In *6th International Conference on Interactive Theorem Proving (ITP)*, volume 9236 of *Lecture Notes in Computer Science*, pages 325–343. Springer, 2015. (Acceptance rate: 30/54=0.55).

[8] Arthur Azevedo de Amorim, Maxime Dénès, Nick Giannarakis, Cătălin Hriţcu, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach. Micro-Policies: Formally verified, tag-based security monitors. In *36th IEEE Symposium on Security and Privacy (Oakland S&P)*, pages 813–830. IEEE Computer Society, May 2015. (Acceptance rate: 55/420=0.13).

[9] Udit Dhawan, Cătălin Hriţcu, Rafi Rubin, Nikos Vasilakis, Silviu Chiricescu, Jonathan M. Smith, Thomas F. Knight, Jr., Benjamin C. Pierce, and André DeHon. Architectural support for software-defined metadata processing. In *20th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pages 487–502. ACM, March 2015. (Acceptance rate: 48/287=0.17).

[10] Arthur Azevedo de Amorim, Nathan Collins, André DeHon, Delphine Demange, Cătălin Hriţcu, David Pichardie, Benjamin C. Pierce, Randy Pollack, and Andrew

Tolmach. A verified information-flow architecture. In *41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 165–178. ACM, January 2014. (Acceptance rate: 51/220=0.23).

[11] Cătălin Hriţcu, John Hughes, Benjamin C. Pierce, Antal Spector-Zabusky, Dimitrios Vytiniotis, Arthur Azevedo de Amorim, and Leonidas Lampropoulos. Testing noninterference, quickly. In *18th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, pages 455–468. ACM, September 2013. (Acceptance rate: 40/133=0.30).

[12] Cătălin Hriţcu, Michael Greenberg, Ben Karel, Benjamin C. Pierce, and Greg Morrisett. All your IFCException are belong to us. In *34th IEEE Symposium on Security and Privacy (Oakland S&P)*, pages 3–17. IEEE Computer Society Press, May 2013. (Acceptance rate: 38/315=0.12).

[13] Michael Backes, Alex Busenius, and Cătălin Hriţcu. On the development and formalization of an extensible code generator for real life security protocols. In *4th NASA Formal Methods Symposium (NFM)*, pages 371–387. Springer, April 2012. (Acceptance rate: 36/93=0.39).

[14] Michael Backes, Cătălin Hriţcu, 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. (Acceptance rate: 24/49=0.49).

[15] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Union and intersection types for secure protocol implementations. In *Theory of Security and Applications (TOSCA 2011; part of ETAPS and the precursor of POST)*, pages 1–28. Springer, March 2011. Invited paper.

[16] Gavin M. Bierman, Andrew D. Gordon, Cătălin Hriţcu, 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. (Acceptance rate: 30/99=0.30).

[17] Michael Backes, Martin P. Grochulla, Cătălin Hriţcu, 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. (Acceptance rate: 22/93=0.24).

[18] Michael Backes, Cătălin Hriţcu, 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. (Acceptance rate: 51/281=0.18).

[19] Michael Backes, Cătălin Hriţcu, 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. (Acceptance rate: 21/115=0.18).

Workshops

[20] Udit Dhawan, Albert Kwon, Edin Kadric, Cătălin Hriţcu, Benjamin C. Pierce, Jonathan M. Smith, Gregory Malecha, Greg Morrisett, Thomas F. Knight, Jr., Andrew Sutherland, Tom Hawkins, Amanda Zyxnfryx, David Wittenberg, Peter Trei, Sumit Ray, Greg Sullivan, and André DeHon. Hardware support for safety interlocks and introspection. In *SASO Workshop on Adaptive Host and Network Security*, September 2012.

[21] Michael Backes, Cătălin Hriţcu, and Thorsten Tarrach. Automatically verifying typing constraints for a data processing language. In *First First International Workshop On Intermediate Verification Languages (BOOGIE 2011)*, July 2011.

[22] Michael Backes, Cătălin Hriţcu, Matteo Maffei, and Thorsten Tarrach. Type-checking implementations of protocols based on zero-knowledge proofs – work in progress. In *Workshop on Foundations of Computer Security (FCS 2009)*, August 2009.

[23] Michael Backes, Martin P. Grochulla, Cătălin Hriţcu, and Matteo Maffei. Achieving security despite compromise using zero-knowledge. In *Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09)*, March 2009.

[24] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Type-checking zero-knowledge. In *Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (FCS-ARSPA-WITS'08)*, June 2008.

[25] Cătălin Hriţcu and Jan Schwinghammer. A step-indexed semantics of imperative objects. In *International Workshop on Foundations of Object-Oriented Languages (FOOL'08)*, January 2008.

Theses

[26] Cătălin Hriţcu. *Union, Intersection, and Refinement Types and Reasoning About Type Disjointness for Security Protocol Analysis*. PhD thesis, Saarland University, January 2012.

[27] Cătălin Hriţcu. A step-indexed semantic model of types for the functional object calculus. Master's thesis, Saarland University, May 2007.

Drafts

[28] Leonidas Lampropoulos, Benjamin C. Pierce, Cătălin Hriţcu, John Hughes, Zoe Paraskevopoulou, and Li-yao Xia. Making our own Luck: A language for random generators. Draft, July 2015.

[29] Yannis Juglaret, Cătălin Hriţcu, Arthur Azevedo de Amorim, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach. Towards a fully abstract compiler using Micro-Policies: Secure compilation for mutually distrustful components. Technical Report, arXiv:1510.00697, October 2015.

[30] Yannis Juglaret, Cătălin Hriţcu, Arthur Azevedo de Amorim, and Benjamin C. Pierce. Beyond full abstraction: Formalizing the security guarantees of low-level compartmentalization. Draft, arXiv:1602.04503, February 2016.

Research Prototypes / Software Tools

2014 – now **F***: Program verification system for ML and proof assistant

2014 – now **Luck**: Domain-specific language for property-based generators for random testing

2013 – now **QuickChick**: Foundational property-based testing plugin for Coq

2011 – 2012 **Breeze**: Language with dynamic information-flow control and label-based access control

2010 – 2011 **DVerify**: Verification tool for the data processing language that served as the main starting point for the query language of Microsoft Power Query for Excel

2009 – 2010 **Dminor**: Type-checker based on semantic subtyping for this data processing language

2009 – 2011 **F5**: Type-checker for concurrent language with refinement, union, and intersection types

2008 – 2011 **Expi2Java**: Turns verifiable protocol models into interoperable Java implementations

2008 – 2011 **zk-typechecker**: First type-checker for protocols that use zero-knowledge proofs

Community Service

PC member for conferences:

- 44th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2017)
- 6th International Conference on Principles of Security and Trust (POST 2017)
- 29th IEEE Computer Security Foundations Symposium (CSF 2016)
- 7th International Conference on Interactive Theorem Proving (ITP 2016)
- 4th ACM-SIGPLAN Conference on Certified Programs and Proofs (CPP 2016)
- 12th International Conference on Applied Cryptography and Network Security (ACNS 2014)

PC member for workshops:

- Workshop on Type-Directed Programming (TyDe 2016)
- 1st International Workshop on Hammers for Type Theories (HaTT 2016)
- Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC 2014)
- 10th Workshop on Foundations of Computer Security (FCS 2013)

Reviewer for journals:
JACM (×1), JCS (×4), TOPLAS (×3), HOSC (×1), JFP (×1), JLAMP (×1)

External reviewer for conferences: Oakland S&P 2016 (×1), PLAS 2014 (×1), POST 2014 (×1), POPL 2014 (×2), CPP 2013 (×1), CSF 2013 (×1), POPL 2013 (×2), CSF 2012 (×1), POST 2012 (×1), ICFP 2011 (×1), CSF 2009 (×4), ISC 2008 (×1), PETS 2008 (×2), ICALP 2008 (×1)

Recent invited presentations

- *Micro-Policies: Formally Verified, Tag-Based Security Monitors.* **Invited speaker** at Workshop on Programming Languages and Analysis for Security (PLAS 2015)
- *More Secure Software Systems by Formal Verification, Property-Based Testing, Secure Compilation, and Dynamic Monitoring.* **Invited vision talk** at scientific committee meeting of Alcatel-Lucent's Bell Labs – Inria common lab (2015).
- *Micro-Policies*: seminars in 2015 at Microsoft Research Redmond, in the DGA (French Department of Defense) seminar on formal methods and security at Inria Rennes, and at HP Labs Paris
- *Dependable Property-Based Testing*: seminars at University of Washington (2015), Université Paris-Sud (2014), Université Paris Diderot – Paris 7 (2014), and Stanford (2013)
- *CRASH/SAFE*: seminars at MSR Cambridge (2013), IFIP Working Group 2.8 – Functional Programming (2012), Harvard University (2012), and Stevens Institute of Technology (2011)

Recent conference and workshop talks

09/2015 *Full dependency and user-defined effects in F*.* ML Workshop 2015.

01/2015 *Foundational Property-Based Testing.* CoqPL Workshop 2015.

07/2014 *Micro-Policies: Formally Verified, Tag-Based Security Monitors.* Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC).

06/2013 *Testing Noninterference, Quickly.* Short talk at IEEE 26th Computer Security Foundations Symposium (CSF).

05/2013 *All Your IFCException Are Belong To Us.* Symposium on Security & Privacy (Oakland)

Recent Teaching

- *F* Tutorials* at POPL 2015, ICFP 2015, and the Joint EasyCrypt-F*-CryptoVerif School 2014.
- *F* Course: Type Systems for Security Verification*, Advanced Block Lecture, Saarland University, together with Matteo Maffei, March 2015 (**main lecturer**, 6 lectures and 6 tutorial sessions).
- *Advanced Martial Arts in Coq*, University of Pennsylvania, Fall 2012 (guest lecturer for 2 lectures).
- *Software Foundations*, University of Pennsylvania, Benjamin C. Pierce, Spring 2012 (teaching assistant and guest lecturer for 6 lectures; **book co-author**).
- *Advanced Topics in Programming Languages*, UPenn, Fall 2011 (guest lecturer for 2 lectures).
- *Practical Aspects of Security*, Advanced Lecture, Saarland University, Michael Backes, 2009 (teaching assistant and guest lecturer for 3 lectures; **best course award**).

Organization

2014 — Main organizer of the Joint EasyCrypt-F*-CryptoVerif School in Paris (over 80 participants)

2012 – 2013 — Organizer of the TOS reading group at UPenn on the interplay between security, programming languages, verification, operating systems, and hardware architecture

Languages

English (proficient, C2), German (upper intermediate, B2), French (intermediate, B1), Italian (elementary, A2), Romanian (native)

References

Benjamin C. Pierce, Professor at University of Pennsylvania
3330 Walnut Street, Philadelphia, PA 19104, USA; Phone: +1 215 898 6222;
E-mail: bcpierce@cis.upenn.edu

Michael Backes, Professor at Saarland University, Max Planck Fellow at MPI-SWS, Director of CISPA, and Vice-coordinator of MMCI
Postfach 15 11 50, D-66041 Saarbrücken, Germany; Phone: +49 681 302 3259;
E-mail: backes@cs.uni-saarland.de

Andrew D. Gordon, Principal Researcher at Microsoft Research Cambridge and Manager of the PPT Group; Professor at University of Edinburgh
21 Station Road, Cambridge CB1 2FB, UK; Phone: +44 1223 479780;
E-mail: adg@microsoft.com

Karthikeyan Bhargavan, Senior Researcher (DR) and leader of the Prosecco team at Inria Paris; 23 avenue d'Italie, Paris 75013, France;
Phone: +33 1 39 63 59 45; E-mail: karthikeyan.bhargavan@inria.fr

Matteo Maffei, Associate Professor at Saarland University
Postfach 15 11 50, D-66041 Saarbrücken, Germany; Phone: +49 681 302 57368;
E-mail: maffei@cs.uni-saarland.de

Greg Morrisett, Dean of Computing and Information Sciences at Cornell University; 105 Bill and Melinda Gates Hall, Hoy Road, Ithaca, NY 04153, USA;
Phone: +1 607 255-9188; E-mail: greg.morrisett@cornell.edu

March 7, 2016