Cătălin Hriţcu

Curriculum Vitae

Contact

INRIA Prosecco team, 23 Avenue d'Italie, 75013 Paris, France

E-mail: catalin.hritcu@gmail.com

Web: http://prosecco.gforge.inria.fr/personal/hritcu/

Research Interests

My research is primarily focused on *developing rigorous formal techniques for solving security problems.* I am particularly interested in:

- formal methods for computer and network security: security protocols, privacy, anonymity, zero-knowledge, information flow control, access control, integrity protection
- programming-languages techniques: rigorous semantics, type systems, verification, automatic testing, formal metatheory, formally certified tools
- design and verification of security-critical systems: reference monitors, microkernel components, electronic voting systems, crypto devices, security-preserving compilers, mobile devices, etc.

Positions

10/2013–now	Researcher (chargé de recherche) at INRIA Paris-Rocquencourt in the Prosecco team
05/2011–09/2013	Research Associate at University of Pennsylvania; DARPA CRASH/SAFE project; Supervisor: Benjamin C. Pierce

Education

06/2007–01/2012	Ph.D. in Computer Science from Saarland University, Saarbrücken, Germany, Summa cum Laude, Advisors: Michael Backes, 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

Grants

10/2015	Ph.D. grant co-financed by DGA and Inria on "Micro-Policies: High-Assurance Hardware-Assisted Security Monitors"

Awards

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

Fellowships and Scholarships

06/2008–04/2011	Ph.D. fellowship from Microsoft Research Cambridge (UK) and the IMPRS-CS
10/2005–05/2008	M.Sc. and then Ph.D. fellowship from the International Max Planck Research School for Computer Science (IMPRS-CS)

Internships

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

2005, 2006, 2007 Google Summer of Code participant with XWiki.org, Paris

Publications

Recent Drafts

[1] Nikhil Swamy, Cătălin Hriţcu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cédric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, and Jean-Karim Zinzindohoue. Dependent types and multi-monadic effects in F*. Draft, Submitted to POPL, July 2015.

[2] 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, Submitted to POPL, July 2015.

[3] Cătălin Hriţcu, Leonidas Lampropoulos, Antal Spector-Zabusky, Arthur Azevedo de Amorim, Maxime Dénès, John Hughes, Benjamin C. Pierce, and Dimitrios Vytiniotis. Testing noninterference, quickly. arXiv:1409.0393; Submitted to Special Issue of Journal of Functional Programming for ICFP 2013, September 2014.

Journals

[4] 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.

[5] 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.

[6] 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

[7] Benjamin C. Pierce, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. *Software Foundations*. Electronic textbook, Version 3.1, July 2014.

Conferences

[8] Zoe Paraskevopoulou, Cătălin Hriţcu, Maxime Dénès, Leonidas Lampropoulos, and Benjamin C. Pierce. Foundational property-based testing. In Christian Urban and Xingyuan Zhang, editors, *6th International Conference on Interactive Theorem Proving (ITP)*, volume 9236 of *Lecture Notes in Computer Science*, pages 325–343. Springer, 2015.

[9] 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)*. IEEE, May 2015. To appear, (Acceptance rate: 55/420=0.13).

[10] 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).

[11] 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).

[12] 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).

[13] 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).

[14] 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 2012)*, pages 371–387. Springer, April 2012. (Acceptance rate: 36/93=0.39).

[15] 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).

[16] 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.

[17] 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).

[18] 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).

[19] 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).

[20] 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

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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

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

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

Selected Talks

up to date list available at http://prosecco.gforge.inria.fr/personal/hritcu/

03/2014 *QuickChick: Property-based testing for Coq.* Coq Working Group at PPS, Paris 7.

Micro-Policies: A Framework for Verified, Hardware-Assisted Security Monitors

07/2014 Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC)

03/2014 Grande Region Security and Reliability Day in Saarbrücken

Testing Noninterference, Quickly

06/2013 Short talk at IEEE 26th Computer Security Foundations Symposium (CFP)

05/2013 Stanford Security Lunch

05/2013 *Formally Verified Privacy-Preserving Distributed Applications.*
INRIA Paris-Rocquencourt.

All Your IFCException Are Belong To Us:

05/2013 IEEE Symposium on Security & Privacy (Oakland)

11/2012 New Jersey Programming Languages and Systems Seminar

11/2012 IFIP WG 2.8 – Functional Programming

10/2012 PL Group, Harvard University

CRASH/SAFE: Clean-slate Co-design of a Secure Host Architecture:

03/2013 Microsoft Research Cambridge

01/2013 Prosecco team at INRIA Paris-Rocquencourt

12/2012 CASED / EC SPRIDE at TU Darmstadt

12/2012 Information Security and Cryptography group at Saarland University

10/2012 *Poison-pills and dynamic information flow control.* PLClub, UPenn.

04/2012 *On the Development and Formalization of an Extensible Code Generator for Real Life Security Protocols.* 4th NASA Formal Methods Symposium (NFM 2012).

11/2011 *Breeze: A Language For Writing Secure Software.* Stevens Institute of Technology.

Union, Intersection, and Refinement Types and Reasoning about Type Disjointness for Analyzing Protocol Implementations:

07/2011 PLClub, University of Pennsylvania

12/2010 MSR-INRIA Joint Centre, Orsay

Semantic Subtyping with an SMT Solver:

09/2010 15th ACM SIGPLAN International Conference on Functional Programming (ICFP 2010)

05/2010 Workshop on Relations and Data Integrity Constraints and Languages (RADICAL 2010), Microsoft Research Cambridge (UK).

08/2009 *Type-checking Implementations of Protocols Based on Zero-knowledge Proofs – Work in Progress.* Workshop on Foundations of Computer Security (FCS 2009).

Achieving Security Despite Compromise Using Zero-knowledge:

07/2009 22th IEEE Symposium on Computer Security Foundations (CSF 2009)

03/2009 Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09)

Type-checking Zero-knowledge:

10/2008 15th ACM Conference on Computer and Communications Security (CCS 2008)

07/2008 Microsoft Research Cambridge (UK)

Automatic Verification of Remote Electronic Voting Protocols:

07/2008 Microsoft Research Cambridge (UK)

06/2008 21th IEEE Symposium on Computer Security Foundations (CSF 2008)

01/2008 *Step-indexed Semantics of Imperative Objects.* Workshop on Foundations of Object-Oriented Languages (FOOL'08).

Teaching

March 2015 Type Systems for Security Verification (main lecturer)
Advanced Block Lecture, Saarland University, together with Matteo Maffei

Fall 2012 *Advanced Martial Arts in Coq* (guest lecturer for 2 lectures)
CIS 670, University of Pennsylvania, instructor: Benjamin C. Pierce

Spring 2012 *Software Foundations* (TA; guest lecturer for 6 lectures; **book co-author**)
CIS 500, University of Pennsylvania, instructor: Benjamin C. Pierce

Fall 2011 *Advanced Topics in Programming Languages* (guest lecturer for 2 lectures)
CIS 670, University of Pennsylvania, instructor: Benjamin C. Pierce

Winter 2010/11 *Security* (guest lecturer for 1 lecture)
Core Lecture, Saarland University, instructor: Michael Backes

Summer 2009 *Practical Aspects of Security* (teaching assistant; guest lecturer for 3 lectures)
Advanced Lecture, Saarland University, instructor: Michael Backes
(best course award)

Winter 2008/09 *Observational Equivalence for Security Protocols* (organizer; advised students)
Seminar, Saarland University, instructor: Michael Backes

Winter 2007/08 *The Analysis of Electronic Voting Protocols* and (organizer; advised students)
The Secure Implementation of Cryptographic Protocols
Seminar, Saarland University, instructor: Michael Backes

Summer 2007 *Introduction to Computational Logic* (teaching assistant)
Core Lecture, Saarland University, instructor: Gert Smolka

Winter 2006/07 *Language-based Security* (teaching assistant; conducted weekly recitation sections)
Advanced Lecture, Saarland University, instructor: Matteo Maffei

Advised Students

03/2015–08/2015 **Yannis Juglaret**. *Towards a Fully Abstract Compiler Using Micro-Policies – Secure Compilation for Mutually Distrustful Components*
(Inria Research Internship; Master's student at Paris 7 and MPRI; starting as my PhD student on DGA/Inria grant in October 2015)

04/2015–08/2015 **Li-yao Xia**. *Integrating Functional Logic Programming with Constraint Solving for Random Generation of Structured Data*
(Inria Research Internship; Master's student at ENS Paris and MPRI)

03/2015–08/2015 **Simon Forest**. *Micro-F⋆ in F⋆*
(Inria Research Internship; Master's student at ENS Paris and MPRI)

03/2014–08/2014 **Arthur Azevedo de Amorim**. *Micro-Policies: Formally Verified, Hardware-Assisted Security Monitors* (Inria Research Internship; PhD student at UPenn)

04/2014–09/2014 **Zoe Paraskevopoulou**. *A Coq Framework For Verified Property-Based Testing*
(Inria Research Internship; now PhD student at Princeton University)

04/2014–09/2014 **Nick Giannarakis**. *Formally Verified Tag-Based Enforcement of Control Flow Integrity* (Inria Research Internship; now PhD student at Princeton University)

10/2011–04/2012 **Sam Panzer & Nick Watson**. *Zephyr: A Content Management System in Breeze*
(Senior design project at University of Pennsylvania)

04/2011 **Alex Busenius**. *Mechanized Formalization of a Transformation from an Extensible Spi Calculus to Java.* (Master's thesis at Saarland University)

08/2010 **Thorsten Tarrach**. *Automatically Verifying "M" Modeling Language Constraints.*
(Master's thesis at Saarland University; now PhD student at IST Austria)

01/2009 **Martin Grochulla**. *Security Despite System Compromise with Zero-Knowledge Proofs.* (Master's thesis at Saarland University; co-advised with Matteo Maffei; now PhD student at MPI-INF)

10/2008 **Alex Busenius**. *Expi2Java – An Extensible Code Generator for Security Protocols.*
(Bachelor's thesis at Saarland University)

10/2008 **Thorsten Tarrach**. *Spi2F# – A Prototype Code Generator for Security Protocols.*
(Bachelor's thesis at Saarland University)

Recent Software Projects

2014 – now **newF⋆**: Next Generation Security Type System (with Karthik Bhargavan, Cédric Fournet, Chantal Keller, Pierre-Yves Strub, Nikhil Swamy, and others)

2013 – now **QuickChick**: Property-Based Testing Plugin for Coq (with Maxime Dénès, John Hughes, Leonidas Lampropoulos, Zoe Paraskevopoulou, and Benjamin C. Pierce)

2013 – now **Micro-Policies**: Formally Verified, Hardware-Assisted Security Monitors (with Arthur Azevedo de Amorim, André deHon, Maxime Dénès, Udit Dhawan, Nick Giannarakis, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach)

2011 – 2013 **CRASH/SAFE**: participated in the clean-slate co-design of a secure architecture, including novel hardware, OS, and programming language (team effort)

2011 – 2012 **Breeze**: a programming language with dynamic information flow control and label-based access control (with Michael Greenberg, Ben Karel, Benoît Montagu, Greg Morrisett, Benjamin C. Pierce, and others)

2010 **DVerify** a verification tool 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 Gavin Bierman and Andy Gordon)

2009 – 2011 **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 – 2011 **zk-typechecker**: the first type-checker for automatically analyzing protocols that use zero-knowledge proofs (with Stefan Lorenz, Kim Pecina and Thorsten Tarrach)

Community Service

PC member: CPP 2016, FCS-FCC 2014, ACNS 2014, FCS 2013

Reviewer for journals:
JACM (×1), JCS (×2), HOSC (×1), JFP (×1), TOPLAS (×1), JLAMP (×1)

External reviewer for conferences:
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)

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

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@mpi-sws.mpg.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), Leader of the Prosecco team at INRIA Paris-Rocquencourt 23 avenue dâĂŹItalie, 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, Professor at Harvard University
33 Oxford Street, 151 Maxwell Dworkin Hall, Cambridge, MA 02138, USA;
Phone: +1 617 495 9526; E-mail: greg@eecs.harvard.edu

September 14, 2015