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: microkernel components, electronic voting systems, crypto devices, security-preserving compilers, mobile devices, etc.

Positions

10/2013–	Chargé de recherche (CR-2) 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

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)
04/2004–09/2004	Socrates-ERASMUS scholarship at Technical University Braunschweig

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

Publications

Journals

[1] 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.

[2] 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.

[3] 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

[4] Benjamin C. Pierce, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. *Software Foundations*. Electronic textbook, 2013.

Conferences

[5] 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).

[6] 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, 2013. (Acceptance rate: 40/133=0.30).

[7] 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 2013)*, pages 3–17. IEEE Computer Society Press, May 2013. (Acceptance rate: 38/315=0.12).

[8] 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).

[9] 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).

[10] 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.

[11] 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).

[12] 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).

[13] 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).

[14] 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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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

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

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

Selected Talks

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

05/2013 *Testing Noniterference, Quickly.* Stanford Security Lunch

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

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* CIS 670, University of Pennsylvania, instructor: Benjamin C. Pierce	(guest lecturer for 2 lectures)
Winter 2010/11	*Security* Core Lecture, Saarland University, instructor: Michael Backes	(guest lecturer for 1 lecture)
Summer 2009	*Practical Aspects of Security* Advanced Lecture, Saarland University, instructor: Michael Backes **(best course award)**	(teaching assistant; guest lecturer for 3 lectures)
Winter 2008/09	*Observational Equivalence for Security Protocols* Seminar, Saarland University, instructor: Michael Backes	(organizer; advised students)
Winter 2007/08	*The Analysis of Electronic Voting Protocols* and *The Secure Implementation of Cryptographic Protocols* Seminar, Saarland University, instructor: Michael Backes	(organizer; advised students)
Summer 2007	*Introduction to Computational Logic* Core Lecture, Saarland University, instructor: Gert Smolka	(teaching assistant)
Winter 2006/07	*Language-based Security* Advanced Lecture, Saarland University, instructor: Matteo Maffei	(teaching assistant; conducted weekly recitation sections)

Advised Students

03/2014–08/2014	**Arthur Azevedo de Amorim**. *Micro-Policies: Formally Verified Low-Level Tagging Schemes for Safety and Security.* (Inria Research Internship; PhD student at UPenn)
04/2014–09/2014	**Zoe Paraskevopoulou**. *QuickChick: Speeding up Formal Proofs with Property-Based Testing.* (Inria Research Internship; student at NTU Athens)
04/2014–09/2014	**Nick Giannarakis**. *Verified Micro-Policies for Stack Protection and Control Flow Integrity* (Inria Research Internship; student at NTU Athens)
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

2011 – now	**CRASH/SAFE**: participated in the clean-slate co-design of a secure architecture, including novel hardware, operating system, and programming language (team effort)
2011 – now	**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: FCS-FCC 2014, ACNS 2014, FCS 2013

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

Other

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 PI 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

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 and Director of Harvard's Center for Research on Computation and Society
33 Oxford Street, 151 Maxwell Dworkin Hall, Cambridge, MA 02138, USA;
Phone: +1 617 495 9526; E-mail: greg@eecs.harvard.edu

May 11, 2014