Santiago Zanella Béguelin

Curriculum vitæ

☎ +34 913 363732 (4115)
📱 +34 625 169873
FAX +34 913 365018
✉ santiago.zanella@imdea.org

February 2011

Personal details

Name	Santiago Zanella Béguelin
Date of birth	8th September 1981 (México DF)
Nationality	Argentine and Mexican
Marital statue	Single
Home address	C/Alonso Cano 30, 2C 28003, Madrid, SPAIN
Work Address	IMDEA Software Institute Facultad de Informática, UPM Campus de Montegancedo S/N 28660 Boadilla del Monte, SPAIN
Homepage	`http://software.imdea.org/~szanella/`

Education

2006-2010	**PhD in Computer Science**, *École Nationale Superiéure des Mines de Paris*, France.
2000–2006	**Licentiateship in Computer Science**, *Universidad Nacional de Rosario*, Argentina. *Grade average 9.8/10* — University best grade average award
1995–1999	**Secondary Degree**, *Instituto Politécnico Superior, Universidad Nacional de Rosario*, Argentina. Specialization in Electronics

PhD thesis

Title	*Formal Certification of Game-Based Cryptographic Proofs*
Supervisor	Gilles Barthe
Description	Most cryptographic proofs are structured as sequences of games and can be formalized by taking a code-centric view of games as probabilistic programs, relying on programming language techniques to justify proof steps. This dissertation presents CertiCrypt, a framework built upon the Coq proof assistant that enables the machine-checked construction and verification of game-based cryptographic proofs. CertiCrypt provides certified tools to reason about the equivalence of probabilistic programs, including a relational Hoare logic, a theory of observational equivalence, verified program transformations, and implementations of common reasoning patterns in cryptography. We formalize for the first time several prominent case studies, including proofs of security of the OAEP and FDH schemes, and Zero-Knowledge Protocols.
Follow-up	Initiated talks with Springer to prepare a book in the IS&C series based on this dissertation.

Licentiateship thesis

Title	*Formal Specification of the MIDP 2.0 Security Model in the Calculus on Inductive Constructions*
Supervisor	Gustavo Betarte and Carlos D. Luna

Description This dissertation presents the first formal specification of the application security model defined by the Mobile Information Device Profile 2.0 for Java 2 Micro Edition. The specification has been formalized in Coq and allows to reason about the security properties of platforms where the model is deployed.

Experience

2010-2011 **Postdoctoral Researcher**, *IMDEA Software Institute*, Spain.

2006-2009 **Graduate Researcher (as a PhD candidate)**,
Microsoft Research-INRIA Joint Centre and INRIA Sophia Antipolis – Méditerranée, France.

2005-2006 **Teaching Assistant**, *Universidad Nacional de Rosario*, Argentina.

- T-312 Data Structures and Algorithms
- T-321 Functional Programming

2004 (6 months) **Undergraduate Researcher**, *INRIA Sophia Antipolis – Méditerranée*, France.
I formalized the GlobalPlatform smart card specification using the B-method, working in close collaboration with industry experts of the GlobalPlatform consortium (whose members include VISA, MasterCard, NTT).

Languages

English **Fluent**

2008 Test of English for International Communication (TOEIC). Score 985/990

2000 First Certificate in English, University of Cambridge. Grade A

French **Fluent**

Lived almost 4 years in France, took several short courses

Spanish **Native Language**

Publications

[1] Gilles Barthe, Benjamin Grégoire, Yassine Lakhnech, and Santiago Zanella Béguelin. Beyond provable security. Verifiable IND-CCA security of OAEP. In *Topics in Cryptology – CT-RSA 2011*, volume 6558 of *Lecture Notes in Computer Science*, pages 180–196, Berlin, 2011. Springer.

[2] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Programming language techniques for cryptographic proofs. In *1st International conference on Interactive Theorem Proving, ITP 2010*, volume 6172 of *Lecture Notes in Computer Science*, pages 115–130, Berlin, 2010. Springer.

[3] Gilles Barthe, Daniel Hedin, Santiago Zanella Béguelin, Benjamin Grégoire, and Sylvain Heraud. A machine-checked formalization of Sigma-protocols. In *23rd IEEE Computer Security Foundations symposium, CSF 2010*, pages 246–260, Los Alamitos, Calif., 2010. IEEE Computer Society.

[4] S. Zanella Béguelin, B. Grégoire, G. Barthe, and F. Olmedo. Formally certifying the security of digital signature schemes. In *30th IEEE symposium on Security and Privacy, S&P 2009*, pages 237–250, Los Alamitos, Calif., 2009. IEEE Computer Society.

[5] G. Barthe, B. Grégoire, and S. Zanella Béguelin. Formal certification of code-based cryptographic proofs. In *36th ACM SIGPLAN-SIGACT symposium on Principles of Programming Languages, POPL 2009*, pages 90–101, New York, 2009. ACM.

[6] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. Formal certification of ElGamal encryption. A gentle introduction to CertiCrypt. In *5th International workshop on Formal Aspects in Security and Trust, FAST 2008*, volume 5491 of *Lecture Notes in Computer Science*, pages 1–19, Berlin, 2009. Springer.

[7] S. Zanella Béguelin. Formalisation and verification of the GlobalPlatform Card Specification using the B method. In *2nd International workshop on Construction and Analysis of Safe, Secure, and Interoperable Smart Devices, CASSIS 2005*, volume 3956 of *Lecture Notes in Computer Science*, pages 155–173. Springer, 2006.

[8] Santiago Zanella Béguelin, Gustavo Betarte, and Carlos Luna. A formal specification of the MIDP 2.0 security model. In *4th International workshop on Formal Aspects in Security and Trust, FAST 2006*, volume 4691 of *Lecture Notes in Computer Science*, pages 220–234. Springer, 2006.