Marco Stronati

Curriculum Vitae

Homepage: http://www.stronati.org
E-mail: marco@stronati.org
Nationality: Italian
Github: http://github.com/paracetamolo

Address: INRIA
2 rue Simone Iff
75012 Paris
France

Current Position

Since January 2017 I'm a Post-Doctoral researcher at INRIA Paris working with Catalin Hritcu in the Prosecco Team. My research currently focuses on the ERC Secomp project on secure compilation.

Education

- **PhD in Computer Science** at École Polytechnique, France. [2012-2015]
  Thesis: *Designing Location Privacy Mechanisms for flexibility over time and space.*
  Supervisors: Catuscia Palamidessi, Konstantinos Chatzikokolakis.
  Graduated with the highest honors (*mention très honorable*).
- **MSc in Computer Science** at University of Pisa, Italy. [2008-2012]
  Thesis: *Differential privacy for relational algebra: improving the sensitivity bounds via constraint systems.*
  Supervisors: Catuscia Palamidessi and Giorgio Levi.
  Grade: 110/110 *cum laude*.
- **BSc of Electronic Engineering** at Università Politecnica delle Marche, Italy. [2005-2008]
  Grade: 108/110.

Experience

- **Post-Doctoral researcher at INRIA, Paris.** 2017
  I'm managing the project Secomp under the direction of Catalin Hritcu. The project goal is to build a secure and verified compiler for a language with undefined behavior (like C) where different programs can be linked together and maintain a level of integrity even when one of them is taken over by an attacker. We are currently working in a compartmentalized variant of a RISC machine, where the isolation between components is guaranteed at the low level by two enforcement mechanisms: Software Fault Isolation and Micropolicies. SFI is an isolation technique purely implemented in software while Micropolicies is a dedicated tagged hardware. Our compiler is developed and formally proved in Coq. I currently supervise the work of 3 undergraduate students.
- **Post-Doctoral researcher at Cornell Tech, New York.** 2016
  My research was focused on two topics, machine learning and genomic privacy, under the direction of prof. Vitaly Shmatikov. My first contribution was the experimental validation of a privacy attack on services offering machine-learning as a service, such as Google Prediction API and Amazon Machine Learning. The resulting paper was published in Oakland'17 (online presentation). My second contribution focused on the information leakage of a family of secure computation protocols developed for genomic data. The work is currently under development.
- **PhD Student at École Polytechnique, France.** 2012-2015
  My research was mainly on privacy enhancing technologies with a particular attention to geolocation applications. The focus of my thesis was the design of location privacy mechanisms able to adapt to the user needs as they change over time and over space. The techniques I developed were formally verified in their guarantees of privacy and quality of service and experimentally tested on a number of real-world datasets. This work resulted in the publication of 4 scientific papers in leading conferences. A sample of the practical impact of my work is the browser extension Location Guard which is currently enjoying good adoption across several major web browsers.

During this period I learned to work with an international community of scientists, to independently manage my work and to effectively present my results. The experimental work was written in OCaml, while the browser extension in Javascript.

- **Research Intern at Florida International University, USA.** January-March 2014
  Part of my PhD was also devoted to the study of how to measure the information leakage of programs and systems using Quantitative Information Flow, a general technique that encompasses privacy. During my visit I collaborated with prof. Geoffrey Smith, one of the leading experts in this field.
- **Research Intern at École Polytechnique, France.** February-October 2012
  During this internship I developed my MSc thesis centered on Differential Privacy and how to use constraints to improve the performance of existing techniques. This work was published in an international workshop and paved the way to my PhD and to my interest for privacy and security.
- **MSc in Computer Science at University of Pisa, Italy.** 2008-2012
  My studies focused on programming languages, concurrency and verification. I developed several small projects among which an interpreter/compiler for a functional language with partial evaluation (written in OCaml), a framework for distributed computation (in Erlang), Model checking of a small car emergency system with SPIN, parser/translator from SCXML to Javascript (in Java). Topics that left a mark of my education are type systems, abstract interpretation/symbolic execution, process calculi and logic programming with constraints.
- **Internship at Université Paris 13.** February-July 2008
  During this internship I discovered functional programming (OCaml) and collaborated on the open source educational software *Marionnet* for virtualization of computer networks.

Distinctions

- Location Guard: a browser extension for location privacy available on Chrome, Firefox and Opera. 90.000 users in 2015 and featured among the best 12 Addons of the year 2015 by Mozilla.
- Recipient of 3-year Doctoral Scholarship Gasparre Le Monge from École Polytechnique. 2012-2015

Additional Information

Programming languages. Very good knowledge of OCaml, Java and Javascript. Fluent in Python, C++. Good knowledge of web technologies, very proficient shell user (Bash,Awk,Sed) and Linux user.
Languages. Italian (native), English (proficient), French (fluent).

Appendix

Research Interests

My research is in the field of privacy, security and program verification.
At the moment my main interest is in extending techniques used in formally verified compilation (e.g. CompCert) to guarantee security properties.
At the same time I keep exploring the privacy implications of machine learning, specifically how to measure and reduce the vulnerability of a system to a membership inference attack.
The main focus of my PhD was designing Differential Privacy mechanisms. The driving application was location privacy but all the methods I developed are applicable to different domains such as statistical databases or website fingerprinting.
At the same time I was also interested in how privacy and security properties can be modeled and measured in terms of Quantitative Information Flow, a technique started from programming languages and extended to more general information theoretic models. Applications range from side channel analysis to machine learning.

Publications

- R. Shokri, M. Stronati, C. Song, V. Shmatikov: *Membership Inference Attacks against Machine Learning Models.* IEEE Symposium on Security and Privacy, Oakland, S&P'17.

- K. Chatzikokolakis, C. Palamidessi, M. Stronati: *Location Privacy via Geo-Indistinguishability.* International Colloquium on Theoretical Aspects of Computing, ICTAC'15

- K. Chatzikokolakis, C. Palamidessi, M. Stronati: *Constructing elastic distinguishability metrics for location privacy.* Privacy Enhancing Technologies Symposium, PoPETS'15.

- K. Chatzikokolakis, C. Palamidessi, M. Stronati: *Geo-indistinguishability: A Principled Approach to Location Privacy.* International Conference on Distributed Computing and Internet Technology, ICDCIT'15.

- K. Chatzikokolakis, C. Palamidessi, M. Stronati: *A Predictive Differentially-Private Mechanism for Mobility Traces.* Privacy Enhancing Technologies Symposium, PETS'14.

- C. Palamidessi, M. Stronati: *Differential Privacy for Relational Algebra: Improving the Sensitivity Bounds via Constraint Systems.* International workshop on Quantitative Aspects of Programming Languages, QAPL 2012:92-105.