

# Marco Guarnieri

Campus Montegancedo UPM, Pozuelo de Alarcón, 28223, Madrid, Spain

☎ (+34) 91-101-2202 ext 4320 | ✉ marco.guarnieri@imdea.org | 🏠 <https://mguarnieri.github.io>

## Education

---

### ETH Zurich

PHD IN COMPUTER SCIENCE

Advisor: Prof. David Basin

Zurich, Switzerland

Oct. 2012 - Jan. 2018

### Università degli Studi di Bergamo

MASTER OF SCIENCE IN COMPUTER ENGINEERING

Advisor: Prof. Stefano Paraboschi

Bergamo, Italy

Sep. 2010 - Jul. 2012

BACHELOR OF SCIENCE IN COMPUTER ENGINEERING

Advisor: Prof. Stefano Paraboschi

Sep. 2007 - Sep. 2010

## Professional Experience

---

### IMDEA Software Institute

ASSISTANT RESEARCH PROFESSOR

Research Areas: Security & Privacy, Information-flow control, Language-based security

Madrid, Spain

Jun. 2019 - PRESENT

RESEARCHER

Research Areas: Security & Privacy, Information-flow control, Language-based security

Apr. 2019 - May 2019

POSTDOCTORAL RESEARCHER

Research Areas: Security & Privacy, Information-flow control, Language-based security

Jul. 2018 - Apr. 2019

### ETH Zurich

POSTDOCTORAL RESEARCHER

Research Areas: Security & privacy, Database security, Information-flow control

Zurich, Switzerland

Feb. 2018 - May 2018

RESEARCH ASSISTANT

Research Areas: Computer security, Databases, Access control

Oct. 2012 - Jan. 2018

### Università degli Studi di Bergamo

RESEARCH ASSISTANT

Research Areas: Access control, Model-driven engineering

Bergamo, Italy

Aug. 2012 - Sep. 2012

### SAP Labs France

R&D INTERN

Research Areas: Security, Static analysis

Sophia Antipolis, France

Jun. 2010 - Sep. 2010

## Conference and Workshop Publications

---

2021

[1] **Marco Guarnieri**, Boris Köpf, Jan Reineke, Pepe Vila  
**Hardware-Software Contracts for Secure Speculation**  
In: *42nd IEEE Symposium on Security and Privacy (S&P 2021)*

[2] Marco Patrignani, **Marco Guarnieri**  
**Exorcising Spectres with Secure Compilers**  
In: *28th ACM Conference on Computer and Communications Security (CCS 2021)*

2020

[3] **Marco Guarnieri**, Boris Köpf, José F. Morales, Jan Reineke, Andrés Sánchez  
**SPECTECTOR: Principled Detection of Speculative Information Flows**  
In: *41st IEEE Symposium on Security and Privacy (S&P 2020)*

[4] Pepe Vila, Pierre Ganty, **Marco Guarnieri**, Boris Köpf  
**CacheQuery: Learning Replacement Policies from Hardware Caches**  
In: *41st ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2020)*

2019

[5] **Marco Guarnieri**, Musard Balliu, Daniel Schoepe, David Basin, Andrei Sabelfeld  
**Information-Flow Control for Database-backed Applications**  
In: *4th IEEE European Symposium on Security and Privacy (EuroS&P 2019)*

2017

[6] **Marco Guarnieri**, Srdjan Marinovic, and David Basin  
**Securing Databases from Probabilistic Inference**  
In: *30th IEEE Computer Security Foundations Symposium (CSF 2017)*

[7] **Marco Guarnieri**, Petar Tsankov, Tristan Buchs, Mohammad Torabi Dashti, and David Basin  
**Test Execution Checkpointing for Web Applications**  
In: *26th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2017)*

[8] Martin Kucera, Petar Tsankov, Timon Gehr, **Marco Guarnieri**, and Martin Vechev  
**Synthesis of Permissive Privacy Enforcement**  
In: *24th ACM Conference on Computer and Communications Security (CCS 2017)*

2016

[9] **Marco Guarnieri**, Srdjan Marinovic, and David Basin  
**Strong and Provably Secure Database Access Control**  
In: *1st IEEE European Symposium on Security and Privacy (EuroS&P 2016)*

2014

[10] **Marco Guarnieri** and David Basin  
**Optimal Security-Aware Query Processing**  
In: *40th International Conference on Very Large Data Bases (VLDB 2014)*

2013

[11] Mario Arrigoni Neri, **Marco Guarnieri**, Eros Magri, Simone Mutti, and Stefano Paraboschi  
**A Model-Driven Approach for Securing Software Architectures**  
In: *10th International Conference on Security and Cryptography - Position Paper (Secrypt 2013)*

[12] **Marco Guarnieri**, Mario Arrigoni Neri, Eros Magri, and Simone Mutti  
**On the Notion of Redundancy in Access Control Policies**  
In: *18th ACM Symposium on Access Control Models and Technologies (SACMAT 2013)*

[13] Angelo Gargantini, **Marco Guarnieri**, and Eros Magri  
**AURORA: AUTomatic ROBustness coverAge Analysis Tool**  
In: *6th IEEE International Conference on Software Testing, Verification and Validation - Testing Tools Track (ICST 2013)*

2012

[14] Mario Arrigoni Neri, **Marco Guarnieri**, Eros Magri, Simone Mutti, and Stefano Paraboschi  
**Conflict Detection in Security Policies using Semantic Web Technology**  
In: *1st International IEEE-AESS Conference in Europe about Space and Satellite Telecommunications - Security Track (ESTEL 2012)*

[15] **Marco Guarnieri**, Eros Magri, and Simone Mutti  
**Automated Management and Analysis of Security Policies using Eclipse**  
In: *7th Italian Workshop on Eclipse Technologies (Eclipse-IT 2012)*

[16] Angelo Gargantini, **Marco Guarnieri**, and Eros Magri  
**Extending Coverage Criteria by Evaluating their Robustness to Code Structure Changes**  
In: *24th International Conference on Testing Software and Systems (ICTSS 2012)*

[17] Francesco Bolis, Angelo Gargantini, **Marco Guarnieri**, Eros Magri, and Lorenzo Musto  
**Model-Driven Testing for Web Applications using Abstract State Machine**  
In: *8th International Workshop on Model-Driven and Agile Engineering for the Web - Short Paper (MDWE 2012)*

[18] Francesco Bolis, Angelo Gargantini, **Marco Guarnieri**, and Eros Magri  
**Evolutionary Testing of PHP Web Applications with WETT**  
In: *4th International Symposium on Search-Based Software Engineering - Graduate Student Track (SSBSE 2012)*

[19] Gabriel Serme, Anderson Santana De Oliveira, **Marco Guarnieri**, and Paul El Khoury  
**Towards Assisted Remediation of Security Vulnerabilities**  
In: *6th International Conference on Emerging Security Information, Systems and Technologies (Securware 2012)*

[20] **Marco Guarnieri**, Eros Magri, Davide Brugali, and Luca Gherardi  
**A Domain Specific Language for Modeling Differential Constraints of Mobile Robots**  
In: *12th International Conference on Autonomous Robot Systems and Competitions (Robotica 2012)*

2011

[21] Angelo Gargantini, **Marco Guarnieri**, and Eros Magri  
**An Eclipse based environment for conformance testing by FSMs**  
In: *6th Italian Workshop on Eclipse Technologies (Eclipse-IT 2011)*

[22] **Marco Guarnieri**, Paul el Khoury, and Gabriel Serme  
**Security vulnerabilities detection and protection using Eclipse**  
In: *6th Italian Workshop on Eclipse Technologies (Eclipse-IT 2011)*

## Other Publications

---

2017

Marco Guarnieri  
**Formal Foundations for Access and Inference Control in Databases**  
Doctoral thesis, Advisor: Prof. David Basin  
ETH Zurich, Switzerland

2012

Marco Guarnieri and Eros Magri  
**Techniques for Conflict Detection and Minimization for Access Control Policies**  
Master thesis, Advisor: Prof. Stefano Paraboschi  
Università degli Studi di Bergamo, Italy

2010

Marco Guarnieri and Eros Magri  
**Sviluppo di un'applicazione Web-based sicura per il data outsourcing**  
(*Development of a secure data outsourcing web application*)  
Bachelor thesis, Advisor: Prof. Stefano Paraboschi  
Università degli Studi di Bergamo, Italy

## Grants and Fellowships

---

2019

**Ayudas Juan de la Cierva - formación** (FJC2018-036513-I)  
Granted to: **Marco Guarnieri**  
Duration: 2020 – 2022  
Amount: 50.000 €  
Funding agency: Ministerio de Ciencia y Innovación

2018

**Intel Strategic Research Alliance: Information Flow Tracking across the Hardware-Software Boundary**  
Principal Investigators: **Marco Guarnieri**, Jan Reineke, Boris Köpf  
Duration: 2018 – 2021  
Amount: 495.000 \$  
Funding agency: Intel Corporation

**Ayudas para la atracción de talento investigador - modalidad 2** (2018-T2/TIC-11732)  
Granted to: **Marco Guarnieri**  
Duration: 2019 – 2023  
Amount: 80.000 €  
Funding agency: Comunidad de Madrid

## Talks

---

2020

ETH Zurich, Invited lecture at Hardware Security course (D-ITET)  
**SPECTECTOR: Principled detection of speculative information flows**, Nov. 2020

Intel Side-channel Academic Program Workshop  
**Hardware-Software Contracts for Secure Speculation**, Sep. 2020

Intel Side-channel Academic Program Tech Talk  
**Hardware-Software Contracts for Secure Speculation**, Jul. 2020

41st IEEE Symposium on Security and Privacy (S&P 2020)

**SPECTECTOR: Principled detection of speculative information flows**, May 2020

Microsoft Research Cambridge, Programming Language Seminar

**CacheQuery: Learning Replacement Policies from Hardware Caches**, Feb. 2020

Italian Conference on CyberSecurity (ITASEC 2020)

**SPECTECTOR: Principled detection of speculative information flows**, Feb. 2020

Workshop on Principles of Secure Compilation (PRISC 2020)

**Exorcising Spectres with Secure Compilers**, Jan. 2020

2019

Microsoft Research Cambridge, Programming Language Seminar

**SPECTECTOR: Principled detection of speculative information flows**, Nov. 2019

Workshop on Foundations of Computer Security 2019 (FCS 2019)

**SPECTECTOR: Principled detection of speculative information flows**, Jun. 2019

4th IEEE European Symposium on Security and Privacy (EuroS&P 2019)

**Information-Flow Control for Database-backed Applications**, Jun. 2019

2nd International workshop on the use of theorem provers for modelling and verification at the hardware-software interface (ENTROPY 2019)

**SPECTECTOR: Principled detection of speculative information flows**, Jun. 2019

Intel Side Channel Academic Program Workshop

**SPECTECTOR: Principled detection of speculative information flows**, Jun. 2019

Ruhr-Universität Bochum

**Principled detection of speculative information flows**, Mar. 2019

2018

CISPA – Helmholtz Center

**Formal foundations for access and inference control in databases**, May 2018

IMDEA Software Institute

**Formal foundations for access and inference control in databases**, Mar. 2018

ABB Corporate Research Center

**Securing databases from probabilistic inferences**, Jan. 2018

2017

Università degli Studi di Padova

**Securing Databases from Probabilistic Inference**, Sep. 2017

MIT, CSAIL seminar

**Securing Databases from Probabilistic Inference**, Sep. 2017

Harvard University, Programming language seminar

**Securing Databases from Probabilistic Inference**, Sep. 2017

Maryland University, Cybersecurity Center seminar,

**Securing Databases from Probabilistic Inference**, Sep. 2017

Stanford University, Formal methods seminar,

**Securing Databases from Probabilistic Inference**, Aug. 2017

30th IEEE Computer Security Foundations Symposium (CSF 2017)

**Securing Databases from Probabilistic Inference**, Aug. 2017

30th IEEE Computer Security Foundations Symposium (CSF 2017)

**Reconciling Database Access Control and Information-flow Control**, Aug. 2017

26th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2017)

**Test Execution Checkpointing for Web Applications**, Jul. 2017

Darmstadt University, Modeling and Analysis of Information Systems Graduate seminar

**Securing Databases from Probabilistic Inference**, Jun. 2017

2016

1st IEEE European Symposium on Security and Privacy (EuroS&P 2016)

**Strong and Provably Secure Database Access Control**, Mar. 2016

2014

40th International Conference on Very Large Data Bases (VLDB 2014)

**Optimal Security-Aware Query Processing**, Sep. 2014

2013

13th International School on Foundations of Security Analysis and Design (FOSAD)

**ActionGUI**, Sep. 2013

18th ACM Symposium on Access Control Models and Technologies (SACMAT 2013)

**On the Notion of Redundancy in Access Control Policies**, Jun. 2013

6th IEEE International Conference on Software Testing, Verification and Validation (ICST 2013)

**AURORA: AUTomatic ROBustness coverage Analysis Tool**, Mar. 2013

2012

7th Italian Workshop on Eclipse Technologies (Eclipse-IT 2012)

**Automated Management and Analysis of Security Policies using Eclipse**, Sep. 2012.

University of Luxembourg, SnT/SRM Research Seminar

**Extending Coverage Criteria by Evaluating their Robustness to Code Structure Changes**, Jul. 2012

ETH Zurich, Information Security group

**Conflict Detection and Minimization Techniques for Access Control Policies**, Jun. 2012

2011

6th Italian Workshop on Eclipse Technologies (Eclipse-IT 2011)

**Security vulnerabilities detection and protection using Eclipse**, Sep. 2011.

## Service

---

2021

**IEEE Symposium on Security and Privacy (S&P 2022)**

Program Committee member

**ACM Conference on Computer and Communications Security (CCS 2022) - Programming languages and formal methods track**

Program Committee member

**Workshop on Principles of Secure Compilation (PriSC 2022-2023)**

Program Chair

**Workshop on Principles of Secure Compilation (PriSC)**

Steering Committee member

**DARPA/ISAT workshop "DOPLR: Data-Oblivious Interdisciplinary Representation"**

Invited member

**Frontiers in Compute Science/Frontier in ICT**

Member of the Editorial Board (Review Editor)

**Workshop on Principles of Secure Compilation (PriSC 2021)**

Program Committee member

**IEEE European Symposium on Security and Privacy (EuroS&P 2021)**

Program Committee member

**IEEE Symposium on Security and Privacy (S&P 2021)**

External reviewer

**Journal of Computer Security**

Reviewer

2020

**ACM SIGSAC Workshop on Programming Languages and Security (PLAS 2020)**

Program Committee member

**IEEE Computer Security Foundations Symposium (CSF 2020)**

Program Committee member

**IEEE European Symposium on Security and Privacy (EuroS&P 2020)**

Program Committee member

**Journal of Computer Security**

Reviewer

2019

**ACM SIGPLAN conference on Systems, Programming, Languages, and Applications: Software for Humanity – OOPSLA track (OOPSLA)**

External reviewer

**French National Research Agency 2019 generic call**

Scientific Expert

## ERC Advanced Grant 2019 Call

Remote referee

## IEEE Transactions on Dependable and Secure Computing (TDSC)

Reviewer

## 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)

External reviewer

2018

## 19th Privacy Enhancing Technologies Symposium (PETS)

External reviewer

## IEEE Transactions on Information Forensics and Security (TIFS)

Reviewer

2017

## ACM Conference on Computer and Communications Security (CCS)

External reviewer

## VLDB Journal

Reviewer

2016

## European Symposium on Research in Computer Security (ESORICS)

External reviewer

## International Conference on Fundamental Approaches to Software Engineering (FASE)

External reviewer

2013

## VLDB Journal

Reviewer

## PhD thesis committees

---

2019

### **Samira Briongos Herrero, Analysis and design of microarchitectural side-channel attacks and countermeasures**

Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Telecomunicación, 29/11/2019

### **Irfan Ul Haq, Lineage Inference of Packed Malware using Binary Code Similarity**

Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros Informáticos, 12/11/2019

## Teaching

---

### **Universidad Politécnica de Madrid**

*Madrid, Spain*

#### LECTURER

Seguridad Informática — Fall 2018–2020

### **ETH Zurich**

*Zurich, Switzerland*

#### TEACHING ASSISTANT

Security Engineering — Autumn 2013–2016

Information Security — Spring 2015, Spring 2018

Design of Digital Circuits — Spring 2017

Informatik für Mathematiker und Physiker — Autumn 2017

### **Università degli Studi di Bergamo**

*Bergamo, Italy*

#### TEACHING ASSISTANT

Object Oriented Programming – Spring 2011–2012

## Mentoring

---

#### PHD STUDENTS

Zilong Wang, IMDEA Software, Fall 2020

#### MASTER STUDENTS

Tristan Buchs, Checkpointing-Based Testing, Master Thesis, ETH Zurich, Fall 2015

Ernst Zachow, Improving the Efficiency of Fuzz Testing Using Checkpointing, Master Thesis, ETH Zurich, Fall 2014

Marco Lazzari, Systematic Testing of TOR, Master Thesis, ETH Zurich, Fall 2014

#### BACHELOR STUDENTS

Andrés Sánchez, Detecting speculative information-flows in large code bases, Universidad Politécnica de Madrid (co-supervised with Manuel Carro), Spring 2019

Javier Lopez Alonso, Formal models for speculative execution, Universidad Politécnica de Madrid (co-supervised with Manuel Hermenegildo), Spring 2019

Mohammed Ajil, Strong and Secure Access Control for PostgreSQL, Bachelor Thesis, ETH Zurich, Spring 2016

#### RESEARCH INTERNS

Andrés Sánchez, Reasoning about speculative execution attacks, IMDEA Software Institute, Fall 2018

Mohamed Moanis Ali, Speculative execution attacks, IMDEA Software Institute, Fall 2019

Ashwin Nambiar, Side-channel attacks, IMDEA Software Institute, Summer 2020

Aarti Kashyap, Hardware-Software Contracts for Undo and Redo Spectre countermeasures, IMDEA Software Institute, Summer 2020

## Honors & Awards

---

2012 **Scholarship of the city of Ciserano**, Italy

2012 **Scholarship of Università degli Studi di Bergamo (best engineering student)**, Italy

2010 **Scholarship of the city of Ciserano**, Italy

2007 **Scholarship of the city of Ciserano**, Italy