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

Summary

Academic career: I am an Associate Research Professor at IMDEA Software (Spain), which I joined as a postdoctoral researcher in July 2018. Before that, I completed a PhD in the Information Security group at ETH Zurich (Switzerland).

Research summary: My research focuses on developing tools and techniques for designing systems with precise security guarantees. During my PhD, I focused on securing database systems. Since joining IMDEA Software, I have focused on building foundations and tools for reasoning about security at the hardware-software boundary and, in particular, on microarchitectural attacks and defenses.

Awards: For my research on formal models for microarchitectural leaks, I received a best paper award at the IEEE Symposium on Security and Privacy 2021, distinguished paper awards at the ACM Conference on Computer and Communication Security (editions 2022, 2023, and 2024), and an Intel Outstanding Researcher award (awarded by Intel to "leading worldwide academic researchers conducting Intel university-sponsored research"). I also received a "Ramon y Cajal" and a "Juan de la Cierva" fellowships, the two most prestigious fellowships for early-career researchers in Spain.

Funding and projects: Overall, I have attracted funding for more than 1M$. I have been a PI in the HascoSec (2021-2024; 300K$) and in the "Information Flow Tracking across the Hardware-Software Boundary" (2018-2021; 495K$) projects funded by Intel Corp. I have also been involved as a researcher in several regional, national, and European projects.

Scientific service (selection): I have served/am serving on the program committee of top-tier security venues like the IEEE Symposium on Security and Privacy, the ACM Conference on Computer and Communication Security, the Usenix Security Symposium, and the IEEE Computer Security Foundations Symposium. I am serving as Program Vice Co-Chair for Usenix Security 2025. I also served as program chair for the Workshop on Principles of Secure Compilation and the Workshop on Programming Languages and Analysis for Security.

Selected publications:

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)*, Best paper award
Motivation: The paper introduces *speculation contracts*: ISA-level formal specifications capturing a processor's security guarantees in a simple, mechanism-independent manner. The paper precisely formalizes under which conditions a processor satisfies a speculation contract and it provides program-level properties formalizing how to leverage a contract's hardware guarantees to achieve global, end-to-end security. The paper also presents the first rigorous proofs of security for a large class of state-of-the-art hardware-level mechanisms for secure speculation.

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)*
Motivation: The paper introduces speculative non-interference, the first semantic characterization of security against speculative execution attacks. This notion, which compares program leakage under different program semantics (*with* and *without* speculative execution), has been adopted and extended by several follow-up works, and the paper is the most cited one on the topic of program analyses for speculative leaks. This paper also presents the first program analysis (implemented in the SPECTECTOR tool) for proving the absence of speculative leaks.

Zilong Wang, Gideon Mohr, Klaus von Gleissenthall, Jan Reineke, **Marco Guarnieri**
Specification and Verification of Side-channel Security for Open Source Processors via Leakage Contracts
In: *30th ACM Conference on Computer and Communications Security (CCS 2023)*, Distinguished paper award
Motivation: The paper presents the first approach for automatically verifying the soundness of timing leakage models against RTL processor designs. This resulted in the the first automated proofs of soundness for timing leakage models and RTL processors, in particular for the Ibex processor (an in-order 3-stage RISC-V processor for embedded applications).

Xaver Fabian, **Marco Guarnieri**, Marco Patrignani
Automatic Detection of Speculative Execution Combinations
In: *29th ACM Conference on Computer and Communications Security (CCS 2022)*, Distinguished paper award
Motivation: The paper develops a framework for composing speculative semantics capturing speculation due to different mechanisms and implements it as part of the SPECTECTOR program analysis tool. The framework allows defining each speculative semantics independently (thus leading to simpler semantics) and deriving SPECTECTOR's soundness w.r.t. the composed semantics from soundness w.r.t. each component (thus maximizing proof reuse).

Education

ETH Zurich — *Zurich, Switzerland*

PhD in Computer Science — *Oct. 2012 - Jan. 2018*

Advisor: Prof. David Basin

Università degli Studi di Bergamo — *Bergamo, Italy*

Master of Science in Computer Engineering — *Sep. 2010 - Jul. 2012*

Advisor: Prof. Stefano Paraboschi

Bachelor of Science in Computer Engineering — *Sep. 2007 - Sep. 2010*

Advisor: Prof. Stefano Paraboschi

Professional Experience

IMDEA Software Institute — *Madrid, Spain*

Associate Research Professor — *Nov. 2024 - PRESENT*

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

Assistant Research Professor — *Jun. 2019 - Oct. 2024*

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

Researcher — *Apr. 2019 - May 2019*

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

Postdoctoral Researcher — *Jul. 2018 - Apr. 2019*

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

ETH Zurich — *Zurich, Switzerland*

Postdoctoral Researcher — *Feb. 2018 - May 2018*

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

Research Assistant — *Oct. 2012 - Jan. 2018*

Research Areas: Computer security, Databases, Access control

Università degli Studi di Bergamo — *Bergamo, Italy*

Research Assistant — *Aug. 2012 - Sep. 2012*

Research Areas: Access control, Model-driven engineering

SAP Labs France — *Sophia Antipolis, France*

R&D Intern — *Jun. 2010 - Sep. 2010*

Research Areas: Security, Static analysis

Conference and Workshop Publications

2025

[1] Xaver Fabian, Marco Patrignani, **Marco Guarnieri**, Michael Backes
Do You Even Lift? Strengthening Compiler Security Guarantees Against Spectre Attacks
In: *52nd ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2025)*

[2] Bo Fu, Leo Tenenbaum, David Adler, Assaf Klein, Arpit Gogia, Alaa R. Alameldeen, **Marco Guarnieri**, Mark Silberstein, Oleksii Oleksenko, Gururaj Saileshwar
AMuLeT: Automated Design-Time Testing of Secure Speculation Countermeasures
In: *30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2025)*

2024

[3] Gilles Barthe, Marcel Böhme, Sunjay Cauligi, Chitchanok Chuengsatiansup, Daniel Genkin, **Marco Guarnieri**, David Mateos Romero, Peter Schwabe, David Wu, Yuval Yarom
Testing side-channel security of cryptographic implementations against future microarchitectures
In: *31st ACM Conference on Computer and Communications Security (CCS 2024)*
Distinguished paper award

[4] Gideon Mohr, **Marco Guarnieri**, Jan Reineke
Synthesizing Hardware-Software Leakage Contracts for RISC-V Open-Source Processors
In: *27th Design, Automation and Test in Europe Conference and Exhibition (DATE 2024)*
Best paper award Nomination

2023

[5] Zilong Wang, Gideon Mohr, Klaus von Gleissenthall, Jan Reineke, **Marco Guarnieri**
Specification and Verification of Side-channel Security for Open Source Processors via Leakage Contracts
In: *30th ACM Conference on Computer and Communications Security (CCS 2023)*
Distinguished paper award, Intel Hardware Security Academic Award Finalist, CSAW Finalist

[6] Oleksi Oleksenko, **Marco Guarnieri**, Boris Köpf, Mark Silberstein
Hide and Seek with Spectres: Efficient discovery of speculative vulnerabilities with random testing
In: *44th IEEE Symposium on Security and Privacy (S&P 2023)*

2022

[7] Xaver Fabian, **Marco Guarnieri**, Marco Patrignani
Automatic Detection of Speculative Execution Combinations
In: *29th ACM Conference on Computer and Communications Security (CCS 2022)*
Distinguished paper award

[8] Sankha Narayan Guria, Niki Vazou, **Marco Guarnieri**, James Parker
ANOSY: Approximated Knowledge Synthesis with Refinement Types for Declassification
In: *43rd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2022)*

2021

[9] **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)*
Best paper award

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

[11] Enrico Bacis, Dario Facchinetti, **Marco Guarnieri**, Marco Rosa, Matthew Rossi, Stefano Paraboschi
I Told You Tomorrow: Practical Time-Locked Secrets using Smart Contracts
In: *16th International Conference on Availability, Reliability and Security (ARES 2021)*

2020

[12] **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)*

[13] 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

[14] **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

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

[16] **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)*

[17] 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

[18] **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

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

2013

[20] 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)*

[21] **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)*

[22] 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

[23] 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)*

[24] **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)*

[25] 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)*

[26] 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)*

[27] 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)*

[28] 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)*
Best paper award

[29] **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

[30] 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)*

[31] **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

2022

Ayudas Ramon y Cajal (RYC2021-032614-I)
Granted to: **Marco Guarnieri**
Duration: 2023 – 2027
Amount: 236.350 €
Funding agency: Ministerio de Ciencia y Innovación

2021

HascoSec: Principled security verification of processors using hardware-software contracts
Principal Investigators: **Marco Guarnieri**, Jan Reineke
Duration: 2021 – 2024
Amount: 300.000 $
Funding agency: Intel Corporation

InferViz: Weighted Inference and Visualization of Insecure Code Paths (Facebook research award: 2021 Privacy Enhancing Technologies)
Principal Investigators: Musard Balliu, **Marco Guarnieri**
Duration: 2021 – 2023
Amount: 100.000 $
Funding agency: Facebook

2019

Ayudas Juan de la Cierva - formación (FJC2018-036513-I)
Granted to: **Marco Guarnieri**
Duration: 2020 – 2022
Amount: 60.416 €
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

Honors & Awards

2024 **Distinguished paper award,** 31st ACM Conference on Computer and Communications Security (CCS 2024)
2024 **Distinguished reviewer award,** 31st ACM Conference on Computer and Communications Security (CCS 2024)
2024 **Finalist,** Intel Hardware Security Academic Award 2023
2024 **Finalist,** CSAW 2024
2024 **Best paper award nomination,** 27th Design Automation and Test in Europe Conference and Exhibition (DATE 2024)
2023 **Distinguished paper award,** 30th ACM Conference on Computer and Communications Security (CCS 2023)
2023 **Top reviewer award,** 30th ACM Conference on Computer and Communications Security (CCS 2023)
2023 **Noteworthy reviewer award,** 32nd Usenix Security Symposium (SEC 2023)
2022 **Distinguished paper award,** 29th ACM Conference on Computer and Communications Security (CCS 2022)
2022 **Intel Outstanding Researcher Award**
2021 **Best paper award,** 42nd IEEE Symposium on Security and Privacy (S&P 2021)
2012 **Scholarship of Università degli Studi di Bergamo (best engineering student)**

Talks

2024

University of British Columbia
Leakage contracts: A foundation for microarchitectural security, Nov. 2024

31st ACM Conference on Computer and Communications Security (CCS 2024)
Testing side-channel security of cryptographic implementations against future microarchitectures, Oct. 2024

KU Leuven
Leakage contracts: A foundation for microarchitectural security, Oct. 2024

Intel Scalable Assurance workshop
HascoSec: Past, Present, and Future, Sep. 2024

ETH Zurich
Leakage contracts: A foundation for microarchitectural security, Sep. 2024

NII Shonan meeting No.215, "Microarchitectural Attacks and Defenses"
Leakage contracts: A foundation for microarchitectural security, Jun. 2024

2023

Intel Scalable Assurance workshop
An update on the HascoSec project – verification, Sep. 2023

Intel Scalable Assurance workshop
An update on the HascoSec project – post-silicon fuzzing, Sep. 2023

Workshop of Foundations of Computer Security (invited keynote)
Principled foundations for microarchitectural security, Jul. 2023

Intel Scalable Assurance workshop
Hide and Seek with Spectres: Efficient discovery of speculative vulnerabilities with random testing, May 2023

2022

Intel Scalable Assurance workshop
Automatic Detection of Speculative Execution Combinations, Sep. 2022

Journées nationales du GDR Sécurité (invited talk)
Principled foundations for microarchitectural security, Jun. 2022

4th SILM workshop on the Security of Software/Hardware Interfaces (invited talk)
Principled foundations for microarchitectural security, Jun. 2022

HackOn – Ciberseguridad @ Universidad Rey Juan Carlos (invited talk)
An overview of cache side-channel attacks, Feb. 2022

2021

Universidad Complutense de Madrid
Hardware-software security contracts - Principled foundations for building secure microarchitectures, Dec. 2021

Dagstuhl Seminar 21481 - Secure Compilation
Contract-aware secure compilation, Dec. 2021

Dagstuhl Seminar 21442 - Ensuring the Reliability and Robustness of Database Management Systems
Database security: Formalization, verification, and testing – Challenges and open questions, Nov. 2021

Intel Side-channel Academic Program Workshop
Hardware-Software Security Contracts - Principled Foundations for Building Secure Speculation Mechanisms , Nov. 2021

Dagstuhl Seminar 21442 – Ensuring the Reliability and Robustness of Database Management Systems
Database security: Formalization, verification, and testing – Challenges and open questions , Nov. 2021

Intel Scalable Assurance Cluster Kickoff
HascoSec: Principled security verification of processors using hardware-software contracts , Oct. 2021

University of Illinois at Urbana Champaign, Hardware Security reading group
Hardware-Software Contracts for Secure Speculation, Jun. 2021

42nd IEEE Symposium on Security and Privacy (S&P 2021)
Hardware-Software Contracts for Secure Speculation, May 2021

Workshop on Principles of Secure Compilation (PriSC 2021)
Contract-aware secure compilation (short talk), Jan. 2021

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

2025

Usenix Security Symposium (SEC 2025)
Program Vice Co-Chair

Workshop on Principles of Secure Compilation (PriSC)
Steering Committee member (2022-now)

Workshop on Programming Languages and Security (PLAS)
Steering Committee member, Steering Committee Chair (2023-now)

IEEE Computer Security Foundations Symposium (CSF)
Steering Committee member, Publication Chair (2023-now)

ACM Conference on Computer and Communications Security (CCS 2025) - Programming languages and formal methods track
Program Committee member

2024

Usenix Security Symposium (SEC 2024)
Program Committee member

ACM Conference on Computer and Communications Security (CCS 2024) - Programming languages and formal methods track
Program Committee member

Workshop on Principles of Secure Compilation (PriSC)
Steering Committee member

Workshop on Programming Languages and Security (PLAS)
Steering Committee member, Steering Committee Chair

IEEE Computer Security Foundations Symposium (CSF)
Steering Committee member, Publication Chair

Evaluation Committee for the SERICS (Security Rights in CyberSpace) project
Evaluator

Evaluation Jury for Dutch Cyber Security Research Paper Award 2024
Evaluator

2023

ACM Conference on Computer and Communications Security (CCS 2023) - Hardware security track
Program Committee member

Usenix Security Symposium (SEC 2023)
Program Committee member

IEEE Computer Security Foundations Symposium (CSF 2023)
Program Committee member

Workshop on Principles of Secure Compilation (PriSC 2023)
Program Chair, Steering Committee member

Dagstuhl seminar 23481 "MAD: Microarchitectural Attacks and Defenses"
Organizer

Programming Language Mentoring Workshop (PLMW@PLDI)
Organizing committee member

Workshop on Programming Languages and Security (PLAS)
Steering Committee member, Steering Committee Chair

IEEE Symposium on Security and Privacy (S&P 2023)
External reviewer

ERC Advanced Grant 2023 Call
Remote referee

2022

IEEE Symposium on Security and Privacy (S&P 2022)
Program Committee member

IEEE Computer Security Foundations Symposium (CSF 2022)
Program Committee member

Workshop on Principles of Secure Compilation (PriSC 2022)
Program Chair, Steering Committee member

IEEE European Symposium on Security and Privacy (EuroS&P 2022)
Program Committee member

SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2022)
Program Committee member

Workshop on Programming Languages and Security (PLAS)
Steering Committee member, Steering Committee Chair

Computer & Security
Reviewer

ACM Transactions on Programming Languages
Reviewer

French National Research Agency 2022 generic call
Scientific Expert

German Research Foundation
Reviewer

2021

ACM Conference on Computer and Communications Security (CCS 2021) - Programming languages and formal methods track
Program Committee member

Workshop on Programming Languages and Security (PLAS 2021)
Program Chair

DARPA/ISAT workshop - DOPLR: Data-Oblivous Interdisciplinary Representation
Invited member

Dagstuhl Seminar 21481 - Secure Compilation
Invited member

Dagstuhl Seminar 21442 - Ensuring the Reliability and Robustness of Database Management Systems
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

Formal Methods in System Design
Reviewer

ERC Advanced Grant 2021 Call
Remote referee

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

2024

Hans Winderix, *Efficient Enforcement Mechanisms for the Preservation of Control-Flow Confidentiality*
KU Leuven, 03/10/2024

Flavien Solt, *Software-inspired techniques for digital hardware security*
ETH Zurich, 06/05/2024

2023

Pietro Frigo, *Exploiting Hardware from Software: an attack-surface analysis*
Vrije Universiteit Amsterdam, 19/12/2023

Andreas Lindner, *Proving Safety and Security of Binary Programs*
KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science, 02/03/2023

2020

José Vila Bausili, *Learning Secrets and Models from Execution Time*
Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros Informáticos, 30/03/2020 (pre-defense)

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 Informatica — Fall 2018–2023

ETH Zurich

Zurich, Switzerland

Teaching Assistant

Security Engineering — Autumn 2013–2016
Information Security — Spring 2015, Spring 2018
Design of Digital Circuits — Spring 2017
Informatik fur 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
Xaver Fabian, CISPA (unofficially co-supervised with Marco Patrignani), Fall 2021
Antonio Zegarelli, IMDEA Software, Spring 2023 (co-supervised with Niki Vazou)
Elvira Moreno, IMDEA Software, Fall 2023
Marco Abbadini, IMDEA Software, Fall 2024 (visiting PhD student from University of Bergamo)

Master Students

Panagiotis Penna, Side-channel attacks on Large Language Models, IMDEA Software Institute, Fall 2024 (co-supervised with Thaleia Dimitra Doudali)
Marco Negro, Microarchitectural fuzzing on RTL processors, IMDEA Software Institute, Fall 2024
Elvira Moreno, Microarchitectural fuzzing on Gem5 simulator, Master Thesis, IMDEA Software Institute, Fall 2022
Antonio Zegarelli, Dynamic policies for information-flow control, Master Thesis, IMDEA Software Institute (co-supervised with Niki Vazou), Fall 2022
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

Eric García, Fuzzing RISC-V Processors for Speculative Leaks, IMDEA Software Institute, Spring 2023
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

David Mateos Romero, Software fuzzing for microarchitectural leaks, IMDEA Software Institute, Summer 2022
Hoang Nguyen, Automated synthesis of hardware-software contracts, IMDEA Software Institute, Spring 2022
Arpit Gogia, Contract-based fuzz testing of CPU simulators, IMDEA Software Institute, Spring 2022
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