

software



science and technology
for developing better software

annual report
2019
software.idea.org



Manuel Carro

Director, IMDEA Software Institute
June 9, 2020

foreword

The text for the 2019 annual report is actually being written during 2020, and it is impossible not to mention the hard times the world is enduring. Little did we suspect that we would be facing a pandemic that would shatter many established social conventions and bring a still not quantified, but surely difficult to overcome, economic crises. In the hope that this situation will soon become an episode of the past and that wounds be healed quickly, let these brief lines be a recognition for those who fought in the front line of the pandemics and also words of support for those who lost a loved one.

The IMDEA Software Institute was created under the umbrella of the Madrid Regional Government. Its main mission is to perform research of the highest quality on the science and technology leading to the creation of reliable, scalable, and secure software. The rationale behind institutions like this is the belief that investing in transformative research is a successful and cost-effective way of generating knowledge, competitiveness, sustainable growth, and employment. Market data and projections support the growing importance of software. Besides the increased presence of software-related news in the media, a study performed at the beginning of 2020 by the global market intelligence firm *International Data Corporation* forecast a global spending of \$4.3 trillion on information and communication technologies for the year 2020 — an increase of over 3.6% over 2019. Information technologies were expected to be responsible for more than a half of this difference, with the sector of application development providing the highest spending growth. While the reliability of predictions depends, specially now, on many unknowns, it is certainly a sign that the presence of software in our lives, and its contribution to the well-being of our society, will continue to be paramount.

The key observation that inspired the design of the IMDEA Software Institute is that researchers and support staff are our main asset. While this is true for any scientific discipline, it is even more relevant in areas where experimentation facilities and research equipment are comparatively less

expensive. Therefore, the Institute continues making efforts towards attracting to Madrid the best possible researchers in a field where competition from academia and industry is rife, to ensure that we fulfill the primary requirement to success in the ICT area. Our researchers and admin staff included, during 2019, 18 faculty member (two part-time and one on leave of absence), 5 visiting and affiliate faculty members, 15 postdoctoral researchers, 3 research programmers, 27 research assistants, 30 interns, 3 project management staff, and 15 support staff members, from more than 32 different nationalities. Our researchers have joined the Institute after working at or obtaining their Ph.D. degrees from prestigious centers, including the U. of Texas at Austin, Stanford U., Carnegie Mellon U., U. of California at San Diego, or Microsoft Research in the US, CWI in the Netherlands, INRIA in France, U. of Cambridge in the UK, the Max Planck Software Institute in Germany, ETH in Switzerland, U. Manchester, or U. Brussels in Europe, to name just a few. In addition, 278 international researchers have visited and given talks at the Institute to date.

During 2019, Institute researchers have published 67 refereed publications in some of the top venues in the field, such as IEEE S&P, CRYPTO, DCC, CAV, PLDI, LICS, PODC, CCS, NIPS, POPL, or OOPSLA — all of them ranked in the A* (the highest) category by CORE, the internationally accepted ranking of computer science conferences and journals. Additionally, the IMDEA Software Institute continued enjoying a very relevant presence in international scientific events. Its researchers gave 8 invited talks in international conferences, 47 invited seminars and lectures, chaired 11 program committees, and participated as members in 38 program committees and 21 boards of journals and steering committees of conferences during 2019. Moreover, 23 best paper awards or distinguished paper mentions were received in the last 5 years.

The Institute has also participated in 23 externally funded research projects and contracts and its researchers enjoyed 15 fellowships during 2019. Twelve of these projects are sponsored by international agencies and companies, six

have direct industrial funding, and seven of them involve collaboration with companies of all sizes, both from Spain and abroad, including, among others, NEC, Intel, Protocol Labs, Toshiba, Adva, Deutsche Telekom, Mellanox, British Telecom, Orange, Thales, Telefónica, Atos, Zemsania, and SENER Aeroespacial.

The Institute continued its EIT Digital role as both partner and host of the Co-Location Center of EIT Digital Spain, the hub where the local activities of EIT Digital take place: startups and scale-ups in the coaching program of EIT Digital have space at the Institute, and activities on innovation, entrepreneurship, and business development for the students of the Master and PhD Schools of EIT Digital happen at IMDEA Software. This creates an environment where synergies among fundamental and applied research, innovation, and entrepreneurship are created in an atmosphere that is difficult to replicate anywhere else.

Last, the Institute made substantial efforts during 2019 to ramp up its dissemination and communication activities with the addition of a communication manager. That led to an increase of presence in social and traditional media, as well as the organization of and participation in more events geared towards making our activities better known by the general public: workshops and fairs for high school students, celebration of the role and the future of girls and women in science, and participation in large science and technology-related events, among others.

I would like to once more thank all who have contributed to the achievements of the Institute so far, including of course the Madrid Regional Government and Assembly for their vision and support, and very specially all the staff of the Institute at all levels. It is their enthusiasm, dedication, and passion that has allowed the Institute go this far in a so short amount of time.

foreword

annual report
2019
software.imdea.org

editor

IMDEA Software Institute

graphic design

base 12 diseño y comunicación

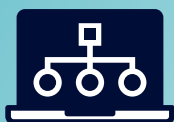
D.L.

M-24122-2020

contents

the institute at a glance	6
motivation and goals	10
legal status, governance, and management	14
members of the governing bodies	22
cooperation	26
research areas	34
research highlights	58
research projects and contracts	74
people	
communication and dissemination	

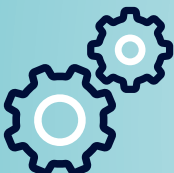
about us



methods



languages



tools

The IMDEA Software Institute is a non-profit, independent research institute promoted by the Madrid Regional Government to perform attraction of talent, research of excellence, and technology transfer in methods, languages and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., software which is **safe, reliable, and efficient**.

The IMDEA Software Institute is part of the Madrid Institutes for Advanced Studies (IMDEA), an institutional framework created to foster **social and economic growth** in the region of Madrid by promoting research of excellence and technology transfer in a number of strategic areas with high potential impact.





Since 2013, the IMDEA Software Institute is located in its headquarters building, at the **Montegancedo Science and Technology Park**. The campus has the “International Campus of Excellence” label and the “Campus of Excellence in Research and Technology Transfer” award from the Spanish government. It is an ideal environment for fulfilling the mission of **attraction of talent, research, and technology transfer**. It is highly energy-efficient, through energy-conscious design, co-generation, and full automation.

The building also provides ample space for strategic activities such as the **Madrid Co-location Center of the EIT Digital KIC** and collaboration activities with companies such as Protocol Labs and NEC.

The location of the IMDEA Software building provides excellent access to the UPM School of Computer Science as well as to the other research centers within the Campus and convenient access to the other Madrid universities and IMDEAs.



the institute at a glance

2019 in figures



researchers



nationalities



PhD thesis

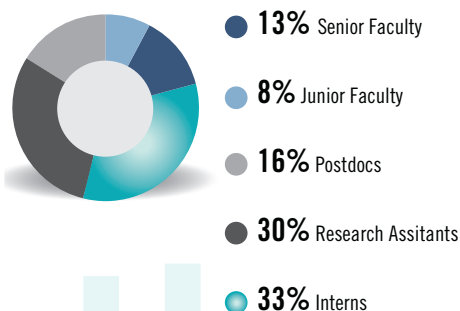


active
fellowships

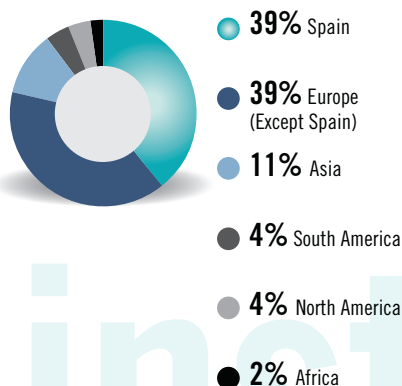


active
projects*

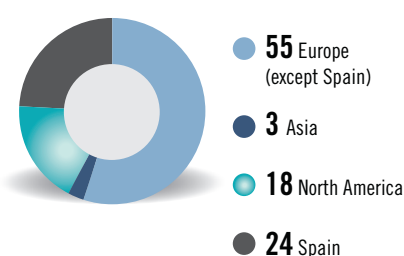
Researchers



Nationalities (all researchers)

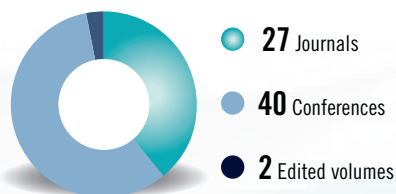


Where Ph.D. was obtained

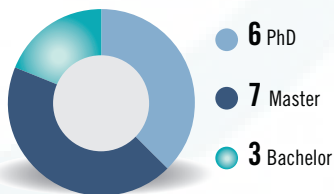


* Three of these projects are industry contracts under non-disclosure agreements whose details cannot be given at the moment.

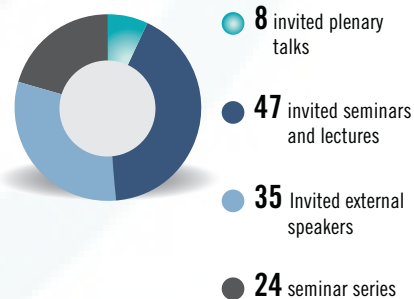
Publications



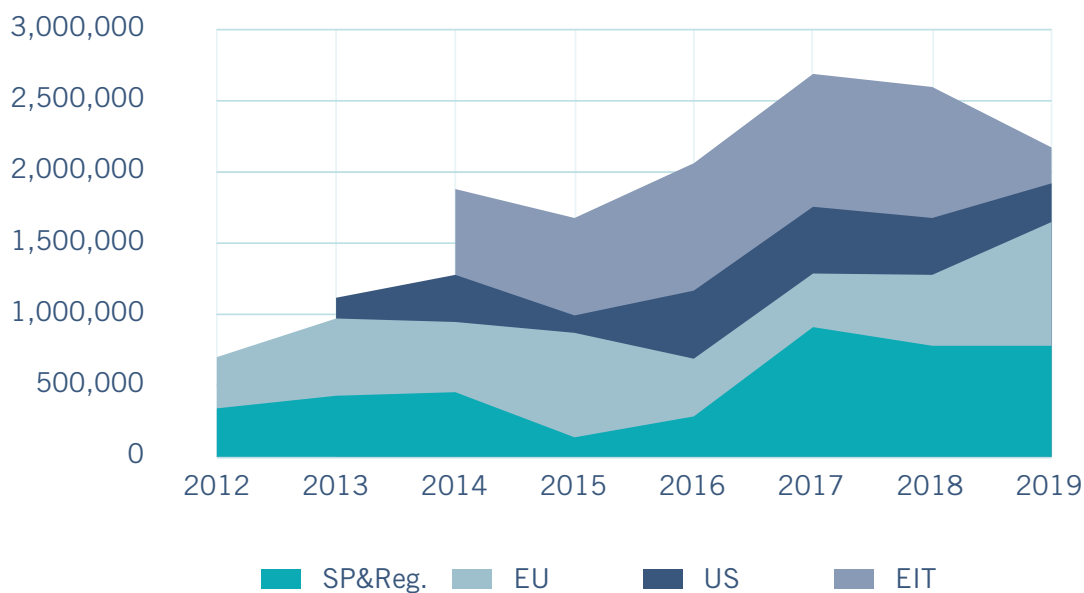
Thesis



Invited Talks



R&I External Income



Accumulated projects & fellowships



Projects
since 2008



Fellowships
since 2008

at a glance

motivation and goals:

the economic landscape of software production

It is difficult to overstate the importance of software in both our daily lives and in the industrial processes that, running behind the scenes, sustain the modern world. Indeed, software is the enabling technology behind many devices and services that are now essential components of our society, ranging from large critical infrastructures on which our lives depend (cars, planes, air-traffic control, medical devices, banking, the stock market, etc.) to all devices that which are now an essential part of our lives (like cell phones, tablets, computers, digital televisions, and the Internet itself). Software has not only facilitated improved solutions to existing problems, but has also started modern revolutions like social networks that change the way we communicate and interact with our environment and with our fellows.

This pervasiveness explains the global figures around software: according to data from the European Commission, the overall software and software-based services (SBSS) market in the EU28 region was worth €229 billion in 2009 and by 2020 it will amount to nearly €290 billion. The average yearly growth of the SBSS industry in Europe is expected to be 2.9% between 2015 and 2020. Software sector employment in the EU grew by 16.1% between 2008 and 2013, as opposed to a decline in employment in the total business economy

of about 3.4%, and high productivity (measured in value added per employee) characterizes the SBSS companies. This vividly illustrates the huge potential of the European SBSS industry to drive economic growth and create jobs. The same source states that approximately half of EU productivity growth comes from investment in ICT, and that the Internet economy creates five new jobs for every two 'offline' jobs lost.

Given the economic relevance of software, it is not surprising that errors, failures and vulnerabilities in software can have high social and economic cost: the results of malfunctioning software can range from being annoying (e.g., having to reboot), through posing serious social and legal problems (e.g., privacy and security leaks), to having high economic cost (e.g., software failures in financial markets and software-related product recalls), or even being a threat to human lives (e.g., a malfunctioning airplane or medical device). A 2013 report from Cambridge University, widely believed to be still applicable today, found that the global cost of debugging software has risen to \$312 billion annually. Moreover, it is estimated that programmers spend at least 50% of their time correcting mistakes (and, in particular, locating the origin of bugs) rather than improving existing code, adding new functionalities, or designing new products.

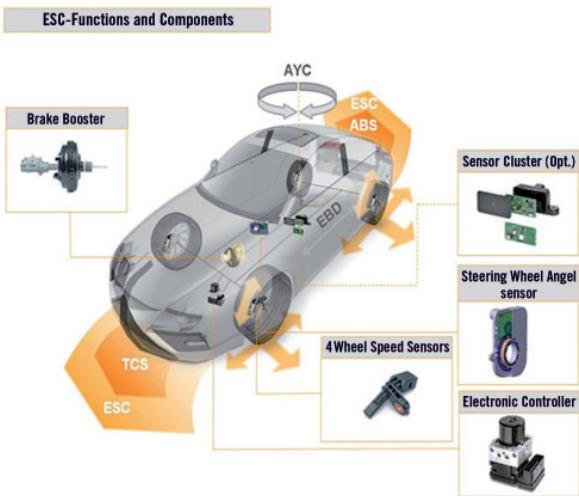
motivation

Other studies estimated the cost to just the U.S. economy at \$60 billion annually, or about 0.6 percent of GDP. The reason for this high cost is that, while some degree of software correctness can be achieved by careful human or machine-assisted inspection, this is still a labor-intensive task requiring highly qualified personnel, with the ensuing high monetary price. Even worse, the risk of errors produced by human mistakes will still be lurking in the dark. Reducing software errors in a cost-effective manner is therefore a task that can greatly benefit from the development of automatic tools.

The security of software systems is also paramount. The European Commission estimates that the damage costs due to cyberattacks in the European Union is in the order of billions each year. Examples of data leaks due to security-related mistakes or malfunctions often appear in the news: in 2013, a data breach in an Internet company leaked birth dates, names, passwords, and email addresses of close to 3 billion subscribers; similarly, data from 500 million customers from a hotel company were stolen from 2014 to 2018; in 2013 a single data breach cost a U.S. retail company \$160 million and more than a 40% drop in its profits.

Developing software technologies that can detect malicious behaviors and provide defense mechanisms against cyberattacks is therefore of primary importance. However, producing automatic tools for reducing software errors as well as developing detection and defense technologies against cyberattacks is extremely hard, because their design and construction poses scientific and technological challenges. At the same time, the ubiquity of software makes taking on these challenges a potentially highly profitable endeavor, since solutions to these problems can have a significant and pervasive impact on productivity, safety, and on the general competitiveness of the economy.

The main mission of the IMDEA Software Institute is to tackle these challenges by performing research of



excellence in methods, languages, and tools that will allow developing software products with sophisticated functionality and high quality, i.e., software products that are at the same time secure, reliable, and efficient, while ensuring that the process of developing such software is also highly cost-effective. A distinctive feature of the Institute is the concentration on approaches that are rigorous and at the same time allow building practical tools. The research focus includes all phases of the development cycle (analysis, design, implementation, verification, validation, evolution and maintenance). In order to achieve its mission, the IMDEA Software Institute gathers a critical mass of world-wide, top-class researchers, and at the same time develops synergies between them and the already significant research base and industrial capabilities existing in the region. Indeed, most of the IT-related companies in Spain (and, specially, their research divisions) are located in the Madrid region, which facilitates collaboration and technology transfer. Thus, the IMDEA Software Institute materializes the opportunity of grouping a critical mass of researchers and industrial experts, allowing for significant improvement in the impact of research and innovation.

and goals



legal status, governance, and management

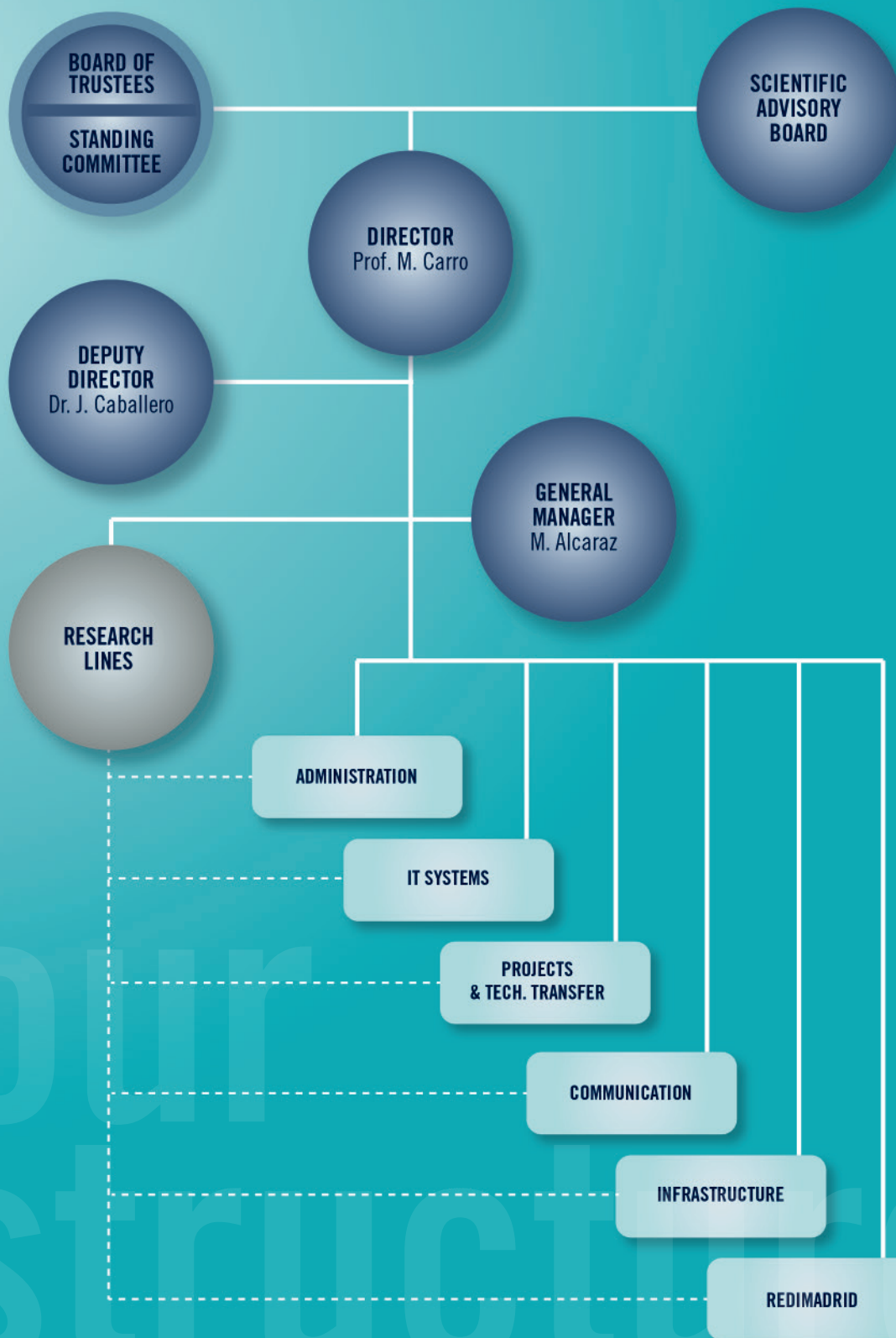
The IMDEA Software Institute is a foundation, which brings together the advantages and guarantees associated with that structure with the flexible and dynamic management more typical of a private body. This combination is deemed necessary to attain the goals of excellence in research, cooperation with industry, and attraction of talented researchers from all over the world, while managing a combination of public and private funds. The Institute was created officially on November 23, 2006 at the initiative of the Madrid Regional Government, following a design that was the result of a collaborative effort between industry and academia, and started its activities during 2007.

The main governing body of the Institute is the **Board of Trustees**. The Board includes representatives of the Madrid Regional Government, universities and research centers of Madrid, scientists with high international reputation in software development science and technology, and representatives of companies, together with independent experts.

The Board is in charge of guaranteeing the fulfillment of the foundational purpose and the correct administration of the funds and rights that make up the assets of the Institute, maintaining their appropriate returns and utility. It normally meets twice a year. In the interim, Board-level decisions are delegated to the **Standing Committee** of

the Board. The **Director**, who is the CEO of the Institute, is appointed by the board among scientists with a well-established international reputation in software development science and technology. The Director fosters and supervises the activities of the Institute, and establishes the distribution and application of the available funds among the goals of the Institute, within the patterns and limits decided by the Board of Trustees. The Director is assisted by the **Deputy Director** and the **General Manager**, who take care of the legal, administrative, and financial activities of the Institute. Together, they supervise the different units in the Institute (administration, IT support, project management, communication, infrastructure, and REDIMadrid) which work closely with and support the **Research** units of the Institute. The current structure is depicted in Figure.

The Board of Trustees and the Director are assisted in their functions by the **Scientific Advisory Board**, composed of high-level external scientists of international reputation with expertise in different areas of research covered by the Institute. The tasks of this advisory board include: to provide advice on and approve the selection of researchers; to provide advice and supervision in the preparation of yearly and longer-term strategic plans; to evaluate the performance with respect to those plans; and to give general advice on matters of relevance to the Institute.





members of the governing bodies

Members of the Board of Trustees and
the Scientific Advisory Board as of Dec. 31st, 2019



BOARD OF TRUSTEES

Chairman of the Foundation

PROF. ROBERTO DI COSMO

Université Paris Diderot and INRIA, France.

Vice-chairman of the Foundation

ILMO. SR. D. EDUARDO SICILIA CAVANILLAS

*Councilor for Science, Universities, and Innovation,
Madrid Regional Government, Spain.*

Regional Government and Public Entities

ILMO. SR. D. EDUARDO SICILIA CAVANILLAS

*Councilor for Science, Universities, and Innovation,
Madrid Regional Government, Spain.*

MARÍA LUISA CASTAÑO MARÍN

*Director-General for Research and Innovation,
Regional Ministry of Science, Universities, and
Innovation, Madrid Regional Government, Spain.*

SARA GÓMEZ MARTÍN

*Director-General for Universities and Higher Art
Studies, Regional Ministry of Science, Universities,
and Innovation, Madrid Regional Government, Spain.*

BÁRBARA FERNÁNDEZ-REVUELTA FERNÁNDEZ-DURÁN

*Deputy Director-General for Research, Regional
Ministry of Science, Universities, and Innovation,
Madrid Regional Government, Spain.*

JOSÉ DE LA SOTA RIUS

*General Coordinator, Fundación para el
Conocimiento madri+d, Madrid, Spain.*

Universities and Public Research Bodies

PROF. NARCISO MARTÍ OLIET

Universidad Complutense de Madrid, Spain.

PROF. JUAN JOSÉ VAQUERO LÓPEZ

Universidad Carlos III de Madrid, Spain.

PROF. FRANCISCO JAVIER SORIANO CAMINO

Universidad Politécnica de Madrid, Spain.

PROF. JESÚS M. GONZÁLEZ BARAHONA

Universidad Rey Juan Carlos, Madrid, Spain.

our structure

SCIENTIFIC ADVISORY BOARD

Scientific Trustees

PROF. ROBERTO DI COSMO

Université Paris Diderot and INRIA, France.

PROF. LUÍS MONIZ PEREIRA

Universidade Nova de Lisboa, Portugal.

PROF. JOSÉ MESEGUER

University of Illinois at Urbana Champaign, USA.

Secretary

ALEJANDRO BLÁZQUEZ LIDOY

Invited Members from Industry

Board meetings have been attended, as invitees, by representatives of the following companies:

Telefónica I+D. *Luis Ignacio Vicente del Olmo, Return on Innovation Manager and Head of Telefónica Patent Office and Estanislao Fernández González-Colaço.*

Atos. *Alicia García Medina, Head of Research & Innovation and Clara Pezuela, Innovation Hub Manager.*

GMV. *Juan José León Cobos, Director of Products and Secure e-Solutions*

Scientific Advisory Board

PROF. ROBERTO DI COSMO

*Université Paris Diderot and INRIA, France.
Chairman of the Board.*

PROF. MARÍA ALPUENTE

Universidad Politécnica de Valencia, Spain.

PROF. VERONICA DAHL

Simon Fraser University, Vancouver, Canada.

PROF. JOSÉ MESEGUER

University of Illinois at Urbana Champaign, USA.

PROF. LUIS MONIZ PEREIRA

Universidade Nova de Lisboa, Portugal.

PROF. MARTIN WIRSING

Ludwig-Maximilians-Universität, München, Germany.

cooperation

Companies with which IMDEA Software Cooperated during 2019



Academic Institutions with which IMDEA Software Cooperated during 2019



Other Publicly-Funded Institutions with which IMDEA Software Cooperated during 2019



Industrial Partnerships

Incorporating scientific results and technologies into processes and products is key to increase the competitiveness of industry. It also contributes to sustainable growth and creates jobs. As a generator of new knowledge in the ICT area, IMDEA Software is committed to the transfer of innovation to industry. *Collaborative projects* (funded through competitive public calls) and *direct industrial contracts* are the key instruments through which collaboration with industry is conducted. Through both, the Institute has established *strategic partnerships* with the main stakeholders in the sector to enable long-term collaboration.

In particular, the Institute has established close ties with Telefónica, Indra, NEC, GMV, SENER Aeroespacial, and Atos, among others, which have led to a number of strategic cooperation initiatives.

An important instance of these initiatives was the creation of the Spanish Associate Partner Group of EIT Digital with Telefónica, Indra, Atos, and UPM that eventually, under the leadership of IMDEA Software, evolved towards the status of Full Node in January 2017. Another instance is the participation of the Institute in the Spanish Network of Excellence on Research on Cyber Security (RENIC) and the European Cyber Security Organization (ECSO) that implements the Cyber Security Public-Private Partnership (cPPP) of the European Commission. All these activities contribute towards aligning research agendas and promote joint participation in projects. A good example of this is the recently granted *MadridFlightOnChip* project, awarded by the Madrid Regional Government, in which IMDEA Software collaborates with companies of the Madrid region working in the aerospace sector.

The currently active projects and contracts are described elsewhere in the report, including a table with the list of companies the Institute has collaborated so far.

Commercialization of Technology

Commercialization of technology is another important form of technology transfer. Given the global controversy around software patents and their legal status in Europe, the Institute combines intellectual property protection with other exploitation models based on licensing. As an example of the former, the Institute routinely performs software registrations of the prototypes developed (e.g., ActionGUI —jointly developed by IMDEA Software and ETH Zurich—, MIST, LEAP, CacheAudit, GGA, and EasyCrypt, ZooCrypt and Masking, these last three developed jointly with INRIA). As an example of the latter, the technology generated through Cadence, an EIT Digital project, was licensed to Communication Valley Reply.



Other Industrial Funding and Collaborations

Other forms of collaboration with industry include the *industrial funding of research assistants* working at the Institute, (e.g., Protocol Labs funds research students working on cryptography), *research stays of Institute researchers at company premises* (e.g., Institute researchers have made industrially-funded extended stays at Microsoft Redmond in the US, Microsoft Cambridge in the UK, Facebook in the UK, Protocol Labs, and elsewhere), *access to the Institute's technology and scientific results* (e.g., researchers of the Institute frequently meet with representatives from the most relevant companies in the IT sector to present research results). In addition, the Institute is open to giving access to the Institute's researchers as consultants and to the participation of company staff in Institute activities.

Academic Partnerships

An important way to cooperate with other academic institutions is through *collaborative projects* funded through competitive calls or industrial contracts. The Institute has also established *longer-term, strategic partnerships* with a number of research institutions in the Madrid region and elsewhere to reach objectives that go beyond those of individual projects. At present the Institute has active long-term agreements with the following universities and research centers:

- Universidad Politécnica de Madrid.
- Universidad Complutense de Madrid.
- Universidad Rey Juan Carlos.
- Universidad Autónoma de Madrid.
- University of Verona, Italy.
- Roskilde University, Denmark.
- Technical University of Cluj-Napoca, Romania.

These agreements establish a framework to develop collaborations that go beyond research projects and include, e.g., the joint development of graduate programs, shared use of resources, equipment, and infrastructure, the association of researchers and research groups with the Institute, or joint commercialization of technology.

As examples that illustrate the importance of these agreements, the agreement with the Universidad Politécnica de Madrid (UPM) included hosting the Institute building in its Montegancedo Science and Technology Park and paves the way for teaching activities at different levels at the School of CS of the UPM, including the supervision of research assistants registered as PhD students at UPM.

Under the agreement with Roskilde University, one of its full professors —John Gallagher— is also part-time senior researcher at the Institute. As mentioned before, the agreement

with ETH Zurich has included the joint development and commercialization of the ActionGUI technology. Finally, the Institute of course also collaborates with the other Institutes in the IMDEA network. As an example, the Institute secured and coordinated the AMAROUT-I and AMAROUT-II COFUND programs of Marie Curie fellowships, which funded personnel in all the IMDEA Institutes, and provides other services to the IMDEA institutes, including hosting a joint coordination unit.

The Institute also has a strong presence in national and international bodies. It is a member of *Informatics Europe*, the organization of all deans, chairs, and directors of the leading Departments and Institutes of Computer Science in Europe. Manuel Hermenegildo, Director of the Institute until mid-2017, was Vice-President of Informatics Europe.

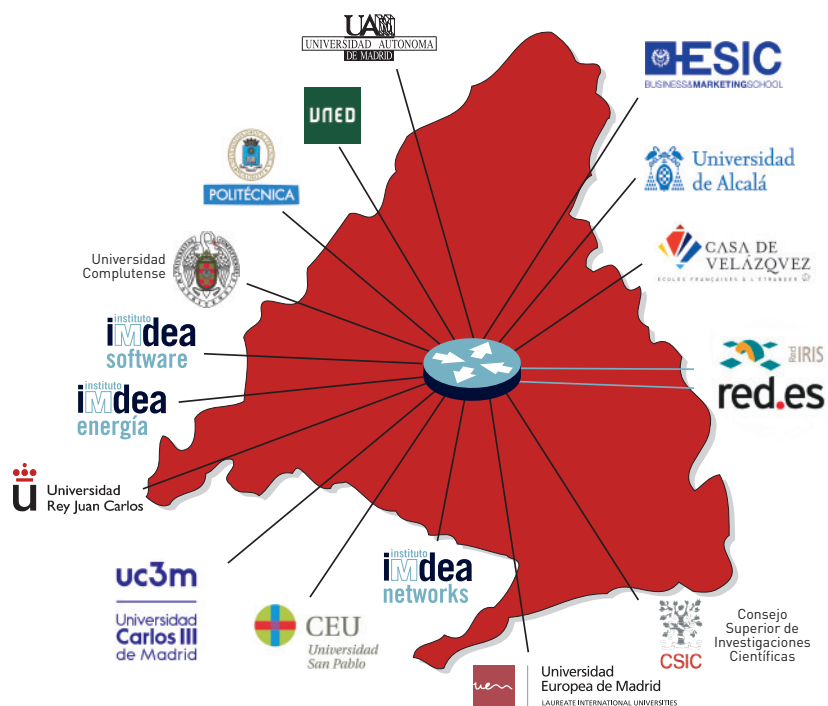
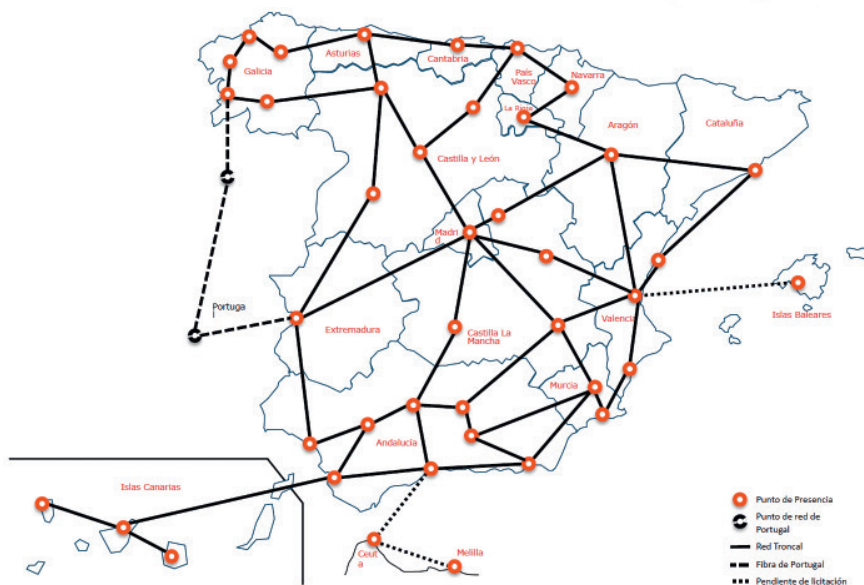
REDIMadrid

REDIMadrid is the data network for research and higher education that provides high-speed connectivity to universities and research centers within the Madrid region. REDIMadrid is funded by the Madrid Regional Government and managed by the IMDEA Software Institute. REDIMadrid provides the connected institutions, which include all public universities in the area of Madrid and the IMDEA research Institutes, with a highly-reliable, high-speed connection. The communication infrastructure provided by REDIMadrid allows these institutions to communicate among themselves and to access the national research network (RedIRIS), the European research network Géant, and the rest of the Internet. Public universities in the area of Madrid are provided diversified connections at a speed at least of 10Gb per second using a physical deployment of metropolitan fiber-optic rings, which provides a highly reliable infrastructure that can be easily updated to new optical and communication technologies.

The *EIT Digital communication node*, hosted and operated by the IMDEA Software Institute, connects to the main points of presence of REDIMadrid using dark fiber acquired by RedIRIS as part of the RedIRIS-NOVA initiative, and operated by REDIMadrid with a pioneering prototype connection of 100Gbps.

In 2019, REDIMadrid continued its expansion with the acquisition of dark fiber that connects the universities in the Ciudad Universitaria Campus (namely, the Universidad Complutense, the Universidad Politécnica, and the UNED) with the points of presence of REDIMadrid (at CIEMAT and CSIC). This continues the plan that started in 2018 with the connection of Universidad Carlos III, IMDEA Networks and Universidad Rey Juan Carlos.



EIT Digital

EIT Digital is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT). EIT Digital (formerly known as EIT ICT Labs) includes some of the leading educational, research, and industrial actors in the ICT innovation ecosystem in Europe, and its mission is to combine educational, research, and industrial tools and activities to drive and foster ICT innovation on the European scale in the following strategic areas: Digital Industry, Digital Cities, Digital Wellbeing, Digital Tech, and Digital Finance. These areas are complemented by integrated and innovation-driven Master and Doctoral Schools, the EIT Digital acceleration programs, and a Professional School.

In June 2013, IMDEA Software officially became an Associate Partner of EIT Digital, becoming the first Spanish organization to enter its Pan-European network of the then seven full national nodes (in Helsinki, Stockholm, Berlin, London, Eindhoven, Paris, and Trento) and two associate nodes (Budapest and Madrid, the latter located at IMDEA Software). Its key goal was to promote, motivate, and organize the presence of EIT Digital in Spain, and to drive the evolution of the Spanish Associate Partner Group (APG) towards a fully operational EIT Digital node. The initial group additionally included Atos, Indra, Telefónica, and the Technical University of Madrid (UPM).

The status of full node, achieved in September 2016, with the start of operations on January 1, 2017, allowed the Madrid Node to have the same rights as the eight other nodes of EIT Digital. This marked the completion of a mission that spanned over the years 2013 to 2016, in which nearly €20 million were invested in Spain. Becoming a Full Node enabled a faster expansion of activities, which undoubtedly happened, as witnessed by the figures for 2019: 45 innovation activity proposals were sent (third node in Europe by number of activities, after Trento and Eindhoven) with a total budget of €12 million, of which 66% was direct EIT funding and the rest was co-funding. It was also the fourth node in academic activities proposed, with 17, with a budget of €2.2 million, 75% of which are direct EIT Digital funding. Likewise, during 2019, the Madrid node was expanded to include as members: BGI, INDRA Business Consulting, INDRA Soluciones Tecnológicas de la Información, INDRA Producción Software, INESC TEC, DTX Colab, GENESIS Biomed, University of Minho, and Worldline.

At the end of the year, EIT Digital partners from the Madrid node participated in 20 innovation activities, in addition to structural and educational ones. All the activities has attracted more than €2.7M of EIT funding to local Spanish partners, of which €2.3M went to innovation and €400K to Education and Training.





Action lines

Digital Industry

Digitised factory, blended retail, personalised products, integrated data-driven process

Digital Infrastructure

The infrastructure itself, convergence of computing and networking; integrated cybersecurity and privacy; built-in intelligence

Digital Cities

Autonomous transportation, open data and city analytics, real/virtual city exploration, safety of the citizens

Digital Finance

Innovative tools and services to help the finance industry adapt to current challenges

Digital Wellbeing

Preventing and coping with physical and cognitive impairments

EIT Digital Co-Location Center

The Co-Location Center of EIT Digital Spain is the central place for organizing and implementing EIT Digital activities in Spain, and the main meeting point for the members of the node. The Madrid CLC continued during 2019 to be located in the building of the Institute, supported by a specific activity aimed at funding the usage and maintenance of the facilities (offices, A/V, meeting spaces, etc.) at the disposal of EIT Digital Spain.

Having the CLC at the headquarters of the Institute makes it possible for the PhD and Master students registered at the EIT-labeled degrees to interact with Institute researchers. Likewise, the startups hosted at the CLC can interact with our researchers and attend the various activities at the Institute (technical talks, workshops, etc).

EIT Digital Accelerator

The Digital Business Developers (BDs) are part of the EIT Digital BD network, and provide a group of 40 specialists helping in bringing ideas to market and providing services such as coaching, access to finance, or soft landing, at a pan-European level. This has also included participation in and organization of events related to innovation and entrepreneurship, some of which took place at the Institute premises and gave the Institute members the possibility to mingle around with representatives of companies and startups and seek ways of collaborating.

EIT Digital Higher Education and Professional Schools

During 2019, the Spanish Node continued the expansion of the EIT Digital Doctoral and the Master School. Several entrepreneurship courses and students working on a daily basis turned the Co-Location Center into a vibrant place for innovation. Additionally, researchers from the IMDEA Software Institute have collaborated in the education schools (in particular, the Professional School) of EIT Digital during 2019.



EIT Digital is supported by the EIT,
a body of the European Union





research areas

The research activities carried out by the IMDEA Software Institute address directly its core mission: to advance the technology and the scientific foundations that enable the cost-efficient development of software for tomorrow's computing platforms. That is, software with sophisticated functionality and high quality in terms of reliability, security, and efficiency. We pursue our mission by focusing on three strategic areas, namely *Program Analysis and Verification*, *Languages, Compilers, and Systems*, and *Security and Privacy*.



Program Analysis and Verification

Our research on *Program Analysis and Verification* advances the theoretical underpinnings and the practical tools that help programmers show, by means of a mathematical proof, that their software executes as intended in terms of functionality, efficiency, and resource consumption.

Establishing program correctness is essential in many existing and emerging industrial domains where malfunctions may have serious negative consequences. Examples include safety-critical avionics and automotive software, embedded and mobile software that must perform within given resource bounds, and electronic currencies and smart contracts, which are essentially a form of programmable money.

In addition to being practically important, proving that software is correct is a source of some of the deepest, most challenging, but also most beautiful scientific and mathematical questions. Here are some of the topics on which IMDEA researchers currently work, and are world-wide leaders.

Verification of concurrent and distributed systems.

- Spatial, temporal, and relational program logics (Hoare logics, separation logic, logics for temporal hyperproperties, logics for information flow security, LTL, CTL).
- Consistency criteria (linearizability, serializability, quiescent linearizability, eventual consistency).
- Weak memory models.
- Consensus algorithms.
- Blockchain and smart contracts.

Formal languages and systems for specification, interactive, and automated proofs.

- Expressive, dependent and higher-order type systems (liquid types, type theories, proof assistants, Coq, Agda).
- Behavioral types (monads, comonads, Hoare types, session types).
- SAT and SMT solvers.

Algorithms and efficient deductive methods for software verification.

- Software model checking, parametrized model checking, automatic abstraction refinement.
- Decision procedures for complex data-types.
- Automata theory and formal languages.

Static analysis and abstract interpretation

- Analysis and verification of software resource consumption (e.g., energy bounds for programs).
- Compile- and run-time assertion checking.
- Automatic refinement of abstract domains.



Languages, Compilers, and Systems

Our research on *Languages, Compilers, and Systems* provides software engineers with the means they need to describe their ideas in more concise and modular ways, and to generate correct and performant executables from these descriptions. Progress in this area has the potential to dramatically increase programmer productivity as well as the maintainability and reusability of software.

IMDEA researchers are world leaders in this quest. Our results include powerful multi-paradigm languages, environments, and techniques that facilitate the programmer's job as well as novel methods for improving program performance. Regarding program correctness and robustness, the aims are similar to those in verification, but the focus here is on tools that find errors and verify programs *during the process of writing such programs*, rather than a posteriori. This focus requires efficient and fully automatic program analysis tools.

The following are some of the research topics that are being explored:

Programming languages and environments

- Multiparadigm programming language theory and implementation. Constraint/logic/functional programming.
- Modern programming features for abstraction, information hiding and code reuse: higher-order, monads, polymorphism, tabling, modules.
- Languages to express and reason with non-monotonic knowledge.
- Combining static and dynamic language characteristics.
- Semantics-based emulation of languages and systems.

Type systems and compiler-based assertion checking

- Type-based program verification, refinement types, liquid types.
- Analysis-based verification of functional and non-functional properties. Assertion languages. Static profiling of resources.

Compilation, transformation, generation

- Resource-aware program transformation and synthesis, partial evaluation.
- Abstract machines, code optimizations, native code generation.
- Auto-parallelization and distribution, with automatic control of resources.

Testing and other dynamic techniques

- Directed testing, random/fuzz testing.
- Run-time verification.

Increased efficiency through the implementation of full systems in hardware

- Pushing computation closer to data.
- Implementation of data movement-intensive stacks (blockchain, distributed algorithms) in reconfigurable hardware.



Security and Privacy

The ever-increasing interconnection, data processing, and storage capabilities enabled by technological advances open up tremendous opportunities for society, the economy, and individuals. At the same time, the digital world is threatened by many kinds of cyberattacks that aim to undermine the security and privacy of digital interactions such as communications, payments, computations, and data storage. These cyberattacks may endanger the economy of our society, but also target important values such as privacy and democracy. Indeed, if the privacy of citizens, governments, and corporations is threatened, this can also impact people's freedom, ultimately creating an imbalance in power relations, which in turn may damage our democratic society.

The research on *security and privacy* at the IMDEA Software Institute aims to deliver technology that enables computation, communication, and storage in open, untrusted, and possibly malicious environments, such as the Internet. Our research results include novel cryptographic protocols and privacy-enhancing technologies, as well as cutting-edge techniques and tools for detecting and analyzing vulnerabilities and malicious activities in software, hardware, and network traffic.

More specifically, our security and privacy research includes:

Cryptography

- Privacy-preserving computation (e.g., homomorphic encryption, functional encryption, multiparty computation).
- Secure outsourcing of data and computation (e.g., verifiable computation, zero-knowledge proofs, homomorphic authentication).
- Privacy in blockchains.

Systems and networks Security

- Defending against malware, cybercrime, and targeted attacks.
- Enhancing software security (e.g., automated testing, vulnerability detection).
- Privacy in the mobile application ecosystem.

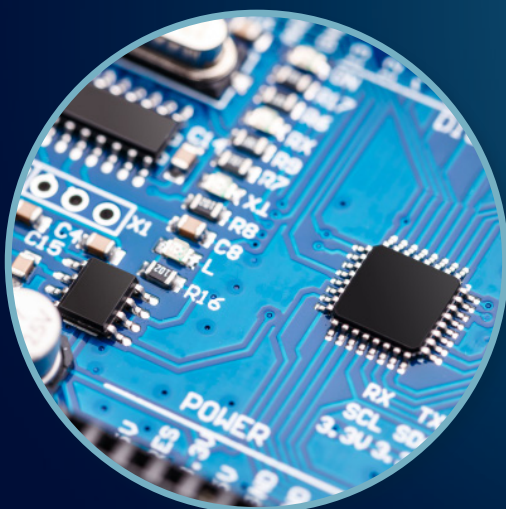
Side-channel attacks and countermeasures

- Detection and analysis of micro-architectural side-channels.
- Compilation and verification of constant-time software defenses.
- Protecting against privacy leaks based on side-channels.





research highlights



**Principled countermeasures
against microarchitectural
CPU attacks**



**Secure Multiparty
Computation**

Principled countermeasures against microarchitectural CPU attacks

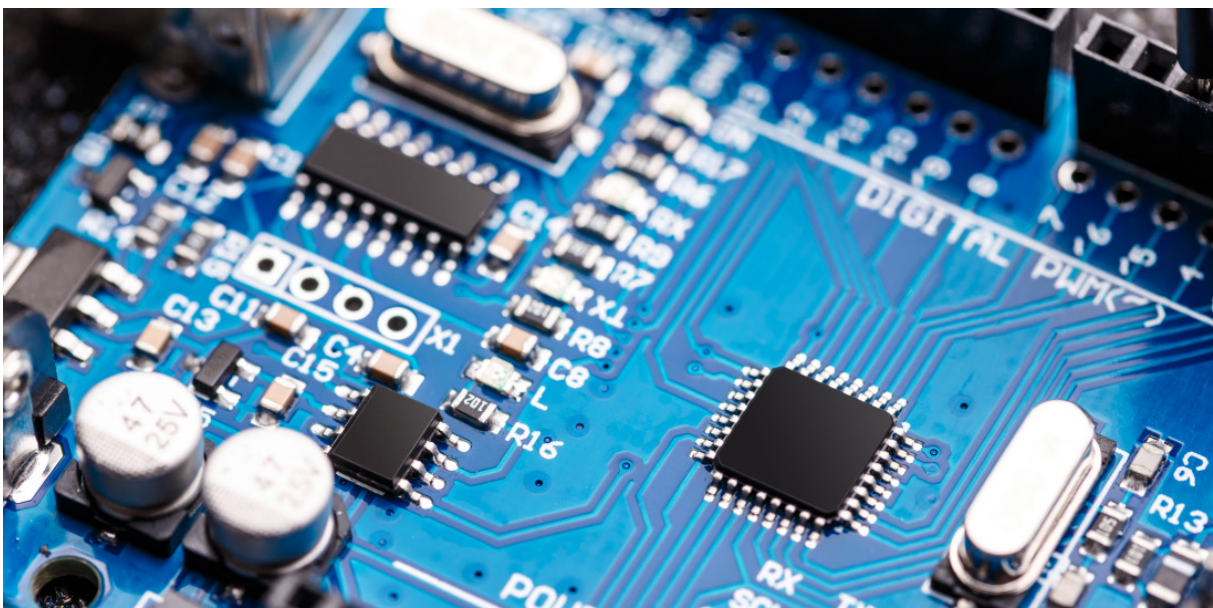
Modern Central Processing Units (CPUs) are complex systems. They employ a multitude of optimizations to achieve high performance. For instance, CPUs might execute instructions in a different order from the one in which they appear in programs to reduce the overall execution time. All these performance-enhancing optimizations are part of the so-called CPU microarchitecture, which describes how instructions are effectively executed by the hardware. Microarchitectural details, however, are transparent to programmers, which interact with CPUs through a high-level interface called the Instruction Set Architecture (ISA). The ISA only specifies the CPU functional behavior and abstracts away from microarchitectural details.

Microarchitectural attacks exploit the gap between the ISA interface and how instructions are actually executed by CPUs to compromise a system's confidentiality and integrity. For instance, an attacker can leak sensitive information by leveraging variations in a program's execution time that result from microarchitectural optimizations. Microarchitectural attacks are critical: even programs that are secure and bug-free at ISA-level can still be vulnerable to such attacks. Moreover, these attacks often affect entire

families of CPUs. As a result, hundreds of thousands of machines are vulnerable to recently discovered microarchitectural attacks such as Spectre (2018), Meltdown (2018), Foreshadow (2018), Ridl (2019), MDS (2019), Spoiler (2019), and ZombieLoad (2019).

Researchers have recently started to develop hardware and software mitigations against different families of microarchitectural attacks. Despite that, proposed countermeasures come with unclear security guarantees and significant performance overhead. Even worse, it is often unclear how programmers can exploit the provided guarantees to write secure programs resistant to microarchitectural attacks.

At our institute, we research tools for better understanding how microarchitectural attacks work and how to defend against them. Towards this, (1) we construct accurate models of microarchitectural components, such as caches and branch prediction units, to better understand the side effects exploited by microarchitectural attacks, (2) we design techniques for reasoning about the effects of microarchitectural attacks, and (3) we develop automated analysis techniques for detecting vulnerable programs and deriving precise security guarantees from programs and countermeasures. Using these models and techniques, we build principled hardware and software countermeasures that provide precise security guarantees against microarchitectural attacks.



Secure Multiparty Computation

Secure multiparty computation studies how to perform privacy-preserving calculations on secret data in a collaborative decentralized manner. In this area of cryptography we consider the scenario where a number of parties, some of which have some information that should be kept private, want to cooperate in order to do some computation that involves this secret data. The goal is therefore that each user learns only the result of the computation but does not get to know the private data from the other parties.

Applications of this technology so far have included domains such as market negotiations with a number of

buyers and sellers, who bid for products but want to keep their bids private to avoid that competitors adapt their strategies; or social studies (e.g. about pay gap between different genders) where private information about citizens can be aggregated and analyzed without the individual data being known by anybody; the same holds for studies about health and genomic data. Future applications can include for example scenarios where smart appliances from several households are able to coordinate their schedules in order to use energy more efficiently, while the consumption profiles are not revealed.



Nevertheless, widespread adoption of secure multiparty computation technologies presents some challenges, perhaps the most important of them being that solutions incur in somewhat large computation times and amount of communication between parties, with respect to how fast these computations would be if the privacy requirements were not present. Another challenging aspect in certain applications is to address the possibility that some of the parties may actively cheat and lead others to wrong outcomes, which is for example a usual concern in applications to blockchain technologies.

At our Institute we are devoting research efforts to minimizing these overheads, using techniques such as pre-processing strategies, amortization mechanisms where we can save complexity if we are performing the same type computation a number of times on different inputs, and optimizing a number of privacy-preserving tools used in secure computation protocols: secret sharing schemes or commitment schemes, all of which require careful manipulations of abstract mathematical notions and structures, for instance finite fields and rings.

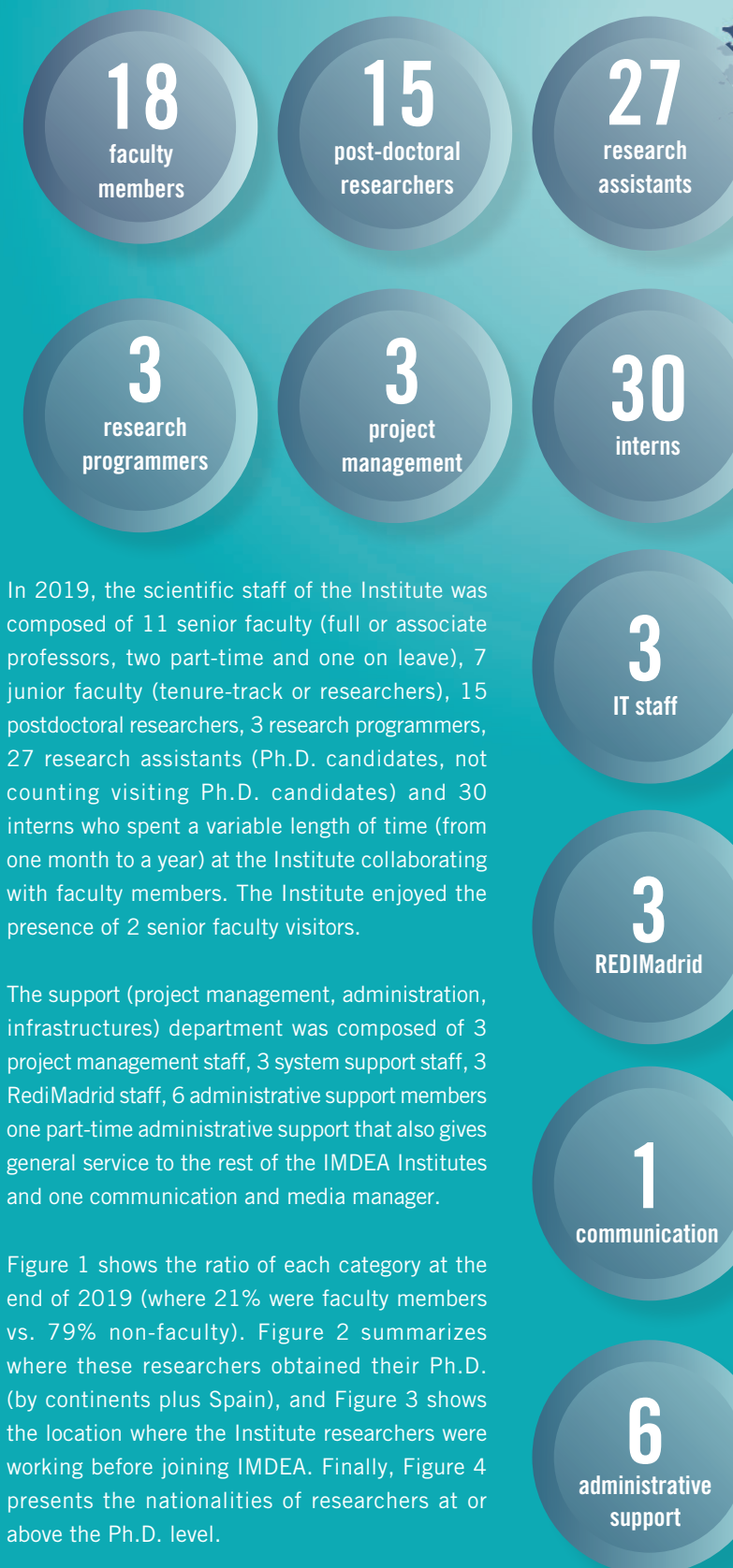


people

The IMDEA Software Institute strives towards the level of excellence and competitiveness of the highest-ranked institutions worldwide. Success in this goal can only be achieved by recruiting highly-skilled personnel for the scientific teams and support staff. The Institute considers this one of the key critical factors and measures of its success.

Competition for talent in Computer Science is extremely high at the international level, since essentially all developed countries have identified the tremendous impact that IT has on the economy and the crucial competitive advantage that attracting truly first class researchers entails. To meet this challenge, the Institute offers a world-class working environment that is competitive with similar institutions in Europe and in the US and which combines the best aspects of a University department and a research laboratory.

Hiring at the Institute follows internationally-standard open dissemination procedures with public, international calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and mailing lists. Appointments at (or promotion to) the Assistant Professor, Associate Professor, and Full Professor levels (i.e., tenure-track hiring, tenure, and promotion decisions) are approved by the Scientific Advisory Board. In addition to faculty positions, the Institute also has its own programs for visiting and staff researchers, post-docs, graduate scholarships, and internships. In all aspects related to human resources, the Institute follows the recommendations of the European Charter for Researchers and a Code of Conduct for their Recruitment (<http://ec.europa.eu/>), which it has duly signed.



In 2019, the scientific staff of the Institute was composed of 11 senior faculty (full or associate professors, two part-time and one on leave), 7 junior faculty (tenure-track or researchers), 15 postdoctoral researchers, 3 research programmers, 27 research assistants (Ph.D. candidates, not counting visiting Ph.D. candidates) and 30 interns who spent a variable length of time (from one month to a year) at the Institute collaborating with faculty members. The Institute enjoyed the presence of 2 senior faculty visitors.

The support (project management, administration, infrastructures) department was composed of 3 project management staff, 3 system support staff, 3 RediMadrid staff, 6 administrative support members one part-time administrative support that also gives general service to the rest of the IMDEA Institutes and one communication and media manager.

Figure 1 shows the ratio of each category at the end of 2019 (where 21% were faculty members vs. 79% non-faculty). Figure 2 summarizes where these researchers obtained their Ph.D. (by continents plus Spain), and Figure 3 shows the location where the Institute researchers were working before joining IMDEA. Finally, Figure 4 presents the nationalities of researchers at or above the Ph.D. level.

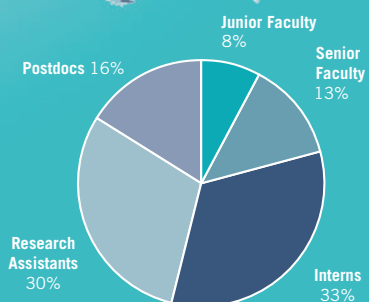


Figure 1. Type of position, all researchers.

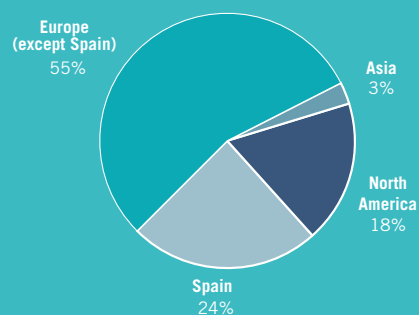


Figure 2. Where Ph.D. was obtained (by continent + Spain).

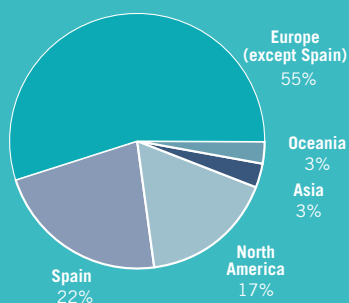


Figure 3. Location of previous institution of researchers at or above postdoc level (by continent + Spain).

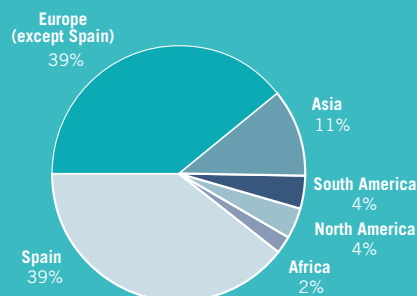


Figure 4. Nationality of researchers at or above PhD level (by continent + Spain).

faculty



Manuel Carro
Associate Research Professor
and Scientific Director

Manuel Carro received his Bachelor degree in Computer Science from the Technical University of Madrid (UPM), and his Ph.D. degree from the same University in 2003. He is currently an Associate Professor at the Technical University of Madrid, Associate Research Professor at the IMDEA Software Institute and, since May 2017, its Director. He is the representative of the Institute at Informatics Europe and at the Node Strategy Committee of EIT Digital Spain. He has previously been Deputy Director at the IMDEA Software Institute, representative of UPM at the NESSI and INES technological platforms, representative of UPM at SpARCIM, deputy representative of IMDEA Software at ERCIM, and CLC Manager and Scientific Coordinator of the Madrid Node of EIT Digital. He has published over 80 papers in international conferences and journals,

and received best paper awards at ICLP 2005 and ICSOC 2011. He has been organizer and PC member of many international conferences and workshops, including conference chair of ICLP 2014 and PC Chair of ICLP 2016, the flagship conference in the field of Logic Programming. He has participated in research projects at the regional, national, and European level. He was UPM's principal investigator for the S-Cube European Network of Excellence and is currently the principal investigator of several national and a regional research projects. He has completed the supervision of five Ph.D. theses.

Research Interests

His interests span several topics, including the design and implementation of high-level (logic- and constraint-based) programming languages to express non-monotonic knowledge and reasoning and to improve the quality of software production, the analysis of service-based systems, and the effective usage of formal specifications in teaching programming. He has long been interested in parallel programming, parallel implementations of declarative languages, and visualization of program execution.



Juan Caballero
Associate Research Professor
and Deputy Director

Juan Caballero received his Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University, USA, in 2010. He joined the Institute in November 2010 as an Assistant Research Professor and was promoted to Associate Research Professor in December 2016. He was appointed Deputy Director of the Institute in September 2017. Prior to joining the Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. Juan also holds an M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH), Sweden, and a Telecommunications Engineer degree from Technical University of Madrid (UPM), Spain. His research regularly appears at the top venues in computer security and has won two best paper awards at the USENIX Security Symposium, a distin-

guished paper award at the ACM Internet Measurement Conference, and the DIMVA Most Influential Paper 2009-2013 award. He is a recipient of the La Caixa fellowship for graduate studies. He has been principal investigator of multiple national and European projects. He has been program chair or co-chair for the ACSAC, DIMVA, DFRWS, ESSOS, and EuroSec conferences, and is a member of the steering committee for ACSAC, DIMVA, and ESSOS. He has been a member of the technical committee for the top computer security venues including IEEE S&P, ACM CCS, USENIX Security, and NDSS.

Research Interests

Juan's research focuses on computer security, including security issues in systems, software, and networks. He designs and implements novel defenses against cybercrime including defenses against malware and software vulnerabilities. He is also interested on big data analysis for security, program binary analysis, and censorship resistance.



Manuel Hermenegildo
Distinguished Professor

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. He joined the Institute on January 1, 2007 as its founding Scientific Director, continuing in this role until May 2017. He is currently Distinguished Professor at the Institute and also Full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining IMDEA Software, he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He was also project leader at the MCC research center and Adjunct Assoc. Prof. at the CS Department of the U. of Texas, both in Austin, Texas, USA. He has received the Julio Rey Pastor Spanish National Prize in Mathematics and Information Science and Technology and the Aritmel National prize in Computer Science, and he is an elected member of the Academia Europaea. He is the president of the Scientific Board of INRIA, member of the Scientific Advisory Board of Dagstuhl, vice-President of Informatics Europe, and member of the Steering Board of EIT Digital, among others. He was also the founding director of the Spanish node of EIT Digital. He has published more than 200 refereed sci-

entific papers and monographs and has given numerous keynotes and invited talks in major conferences. He has also been coordinator and/or principal investigator of many international and national projects, area editor of several journals, and chair and PC member of numerous conferences. He served as General Director for the Spanish national research funding agency, as well as a member of the European Union's high-level advisory boards in information technology (ISTAG, CREST), the board of directors and the scientific board of the Spanish Scientific Research Council (CSIC) and of the Center for Industrial and Technological Development (CDTI), among other national and international duties.

Research Interests

His areas of interest include global program analysis, optimization, verification, and debugging (including resources such as energy and other non-functional properties); abstract interpretation; partial evaluation; parallelism and parallelizing compilers; constraint/logic/functional programming language design and implementation; abstract machines; automatic program documentation; and sequential and parallel computer architecture.



Gilles Barthe
Research Professor (part-time)

Gilles Barthe received a Ph.D. in Mathematics from the University of Manchester, UK, in 1993, and an *Habilitation à diriger les recherches* in Computer Science from the University of Nice, France, in 2004. He has published extensively in programming languages, security, privacy, and cryptography, and was awarded the Best Paper Awards at CRYPTO 2011, PPOPP 2013, and FSE 2016.

He was an invited speaker at numerous venues, including CAV 2016, CSF 2014, ESORICS 2012, ETAPS 2013, EUROCRYPT 2017, IJCAR 2016. He has been coordinator/principal investigator of many national and European projects, and served as the scientific coordinator of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices (2005-2009). He is a member of the editorial board of the Journal of Automated Reasoning and of the Journal of Computer Security.

Research Interests

Gilles' research is currently focused on building foundations for computer-aided cryptography and privacy and on the development of tools for proving the security of cryptographic constructions and differentially private computations.



John Gallagher
Research Professor (part-time)

John Gallagher received the B.A. (Mathematics with Philosophy) and Ph.D. (Computer Science) degrees from Trinity College Dublin in 1976 and 1983 respectively. He held a research assistantship in Trinity College (1983-4), and post-doc appointments at the Weizmann Institute of Science, Israel (1987 - 1989) and Katholieke Universiteit Leuven, Belgium (1989). From 1984-1987 he was employed in research and development in a software company in Hamburg, Germany. Between 1990 and 2002 he was a lecturer and later senior lecturer at the University of Bristol, UK. Since 2002, he has been a professor at the University of Roskilde, Denmark in the research group Programming, Logic and Intelligent Systems and the interdisciplinary Experience Lab and holds a dual appointment at IMDEA Software Institute since February 2007. He chaired the program committee of several international conferences and been a member of the program committee of about 60 others. He has also been in executive committee of the Association for Logic Programming, the steering committee of the ACM SIGPLAN workshop on Partial Evaluation and Program Manipulation and is currently in the steering committee of the Interna-

tional Symposium on Functional and Logic Programming. He has published approximately 60 peer-reviewed articles which have over 2000 citations.

Research Interests

His research interests focus on program specialization, constraint logic programming, rewrite systems, static analysis of software including analysis of energy consumption and other resource properties of programs, automatic software verification, temporal logics, and semantics-based emulation of languages and systems, and has participated in and led a number of national and European research projects on these topics.



César Sánchez
Associate Research Professor

César Sánchez received a Ph.D. degree in Computer Science from Stanford University, USA, in 2007. His thesis studies the applications of formal methods for guaranteeing deadlock freedom in distributed algorithms. After a post-doc at the University of California at Santa Cruz, USA, César joined the IMDEA Software Institute in 2008. He became a Scientific Researcher at the Spanish Council for Scientific Research (CSIC) in 2009. In 2013, he was promoted to Associate Professor at the IMDEA Software Institute.

César holds a degree in Ingeniería de Telecomunicación (MSEE) from the Technical University of Madrid (UPM), Spain, granted in 1998. Funded by a Fellowship from La Caixa, he moved to Stanford University, USA, receiving an M.Sc. in Computer Science in 2001, specializing in Software Theory and Theoretical Computer Science. César was the recipient of the 2006 ACM Frank Anger Memorial Award, and he enjoyed a Juan De La Cierva Fellowship between 2008 and 2009.

Research Interests

César's general research interests are the applications of logic, games and automata theory for the development, the understanding, and the verification of computational artifacts. In particular, César's main line of research is the use of formal methods for reactive systems with emphasis on concurrent, embedded and distributed systems. His foundational research includes the temporal verification of concurrent datatypes and distributed systems, runtime verification and applications, and rich specification languages for modern complex software.



Pierre Ganty
Associate Research Professor

Pierre holds a joint Ph.D. degree in Computer Science from the University of Brussels, Belgium and from the University of Genova, Italy. Prior to join the IMDEA Software Institute in 2009 he did a nearly two-year postdoc at the University of California, Los Angeles. Pierre is associate research professor at the IMDEA Software Institute since late 2015. He is the recipient of a Ramón y Cajal fellowship.

Research Interests

Pierre is interested in fundamental computational problems arising in automated verification of systems with infinitely many states. Recently, he focused on algorithms to decide the containment problem between formal languages of finite and infinite words, a fundamental problem arising in model-checking. He is interested in the application of abstract interpretation to decide those problems.



Aleks Nanevski
Associate Research Professor

Aleks Nanevski obtained his Ph.D. in Computer Science from Carnegie Mellon University, and held postdoctoral research positions at Harvard University and Microsoft Research in Cambridge, before joining IMDEA in 2009. He is a recipient of Ramon y Cajal award in 2010, and an ERC consolidator grant in 2016.

Research Interests

Aleks' researches how to use type-theory to develop and structure mathematical proofs of programs correctness, especially of programs utilizing shared-memory concurrency. Structuring proofs builds on the philosophy of structured programming, to identify linguistic concepts that are frequently used in the practice of formal proving, but are arguably harmful. Such concepts should be replaced by better ones that provide proofs with more structure, and improve on the proof's conciseness, readability, development effort and maintainability, just like structured programming improved the very same aspects of programming. Ultimately, these ideas will enable software development practice where verifying that one's programs works correctly will be a simple, natural, and expected process.



Alexey Gotsman
Associate Research Professor

Alexey Gotsman received his Ph.D. degree in Computer Science from University of Cambridge, UK in 2009. His Ph.D. thesis received a Best Dissertation Award of the European Association for Programming Languages and Systems (EAPLS). Alexey was a postdoctoral fellow at Cambridge before joining IMDEA in September 2010. He is a recipient of a Ramón y Cajal fellowship, and an ERC Starting Grant.

Research Interests

Alexey's research interests are at the intersection of distributed computing and formal verification.



Dario Fiore
Associate Research Professor

Dario Fiore received his Ph.D. degree in Computer Science from the University of Catania, Italy in 2010. Prior to joining the IMDEA Software Institute in November 2013, Dario held postdoctoral positions at Max Planck Institute for Software Systems (Germany), New York University (USA), and École Normale Supérieure (France). During his Ph.D., he was also a visiting student at the IBM T.J. Watson research center and the New York University (USA). He is the recipient of a Juan de la Cierva Incorporación fellowship awarded in 2015.

Research Interests

Dario's research interests are on theoretical and practical aspects of cryptography and its applications to security and privacy in real-world systems. His research focuses on designing provably-secure cryptographic protocols, and his recent work has particular emphasis on developing novel paradigms for the security of data during computation. More specifically, some of the topics he works on include: secure delegation of data and computation to the cloud, homomorphic authenticators, zero-knowledge proof systems, homomorphic encryption, functional encryption, and foundations of cryptography.



Alessandra Gorla
Assistant Research Professor

Alessandra Gorla received her Bachelor's and Master's degrees in computer science from the University of Milano-Bicocca in Italy. She completed her Ph.D. in informatics at the Università della Svizzera Italiana in Lugano, Switzerland in 2011. In her Ph.D. thesis she defined and developed the notion of Automatic Workarounds, a self-healing technique to recover Web applications from field failures, a work for which she received the Fritz Kutter Award for the best industry-related Ph.D. thesis in computer science in Switzerland. Before joining IMDEA Software Institute in December 2014 as an assistant research professor, she has been a postdoctoral researcher in the software engineering group at Saarland University in Germany. During her postdoc, she has also been a visiting researcher at Google in Mountain View.

Research Interests

Alessandra's research interests are in software engineering, and in particular on testing and analysis techniques to improve the reliability and security of software systems. She is also interested in malware detection for mobile applications.

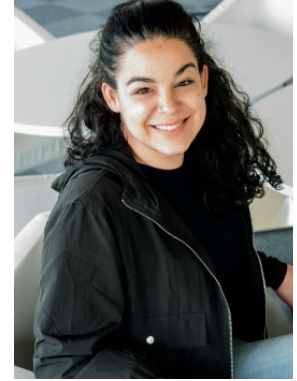


Zsolt István
Assistant Research Professor

Zsolt received his PhD Degree in 2018 from ETH Zürich, Switzerland. His dissertation, entitled "Building Distributed Storage with Specialized Hardware", was awarded with the prestigious ETH Medal by the university. Before joining IMDEA Software as an Assistant Research Professor, he worked as a visiting researcher at IBM Rüschlikon, Switzerland. Prior to his doctoral studies, he completed the Master's degree in Computer Science (Distributed Systems) at ETH Zürich, Switzerland, in 2013, and the Bachelor's degree in Computer Science at UT Cluj-Napoca, Romania, in 2011.

Research Interests

Zsolt's research interests are in using specialized hardware to speed up distributed systems and databases without increasing their energy footprint, and to explore hybrid architectures for emerging data-intensive workloads. He uses field programmable gate arrays (FPGAs) as a vehicle for prototyping ideas.



Niki Vazou
Assistant Research Professor

Niki Vazou obtained her Ph.D. in Computer Science from University of California, San Diego in 2016 and held a postdoctoral fellow position at University of Maryland, College Park. In 2018 Niki joined IMDEA as a Research Assistant Professor. Niki received an MSR graduate research fellowship in 2014 and is a member of the Haskell.org committee since 2016. She has published in many programming languages conferences (e.g., POPL, ICFP, and OOPSLA) and received the Best Paper Award at OOPSLA 2018. Niki has been an invited speaker at research and industrial conferences including Zurichac and Haskell eXchange.

Research Interests

Niki's interests include refinement types, automated program verification, and type systems, and her goal is to make theorem proving a useful part of mainstream programming. She developed Liquid Haskell, an SMT-based, refinement type checker for Haskell programs that has been used for various applications ranging from fully automated light verification of Haskell code (e.g., bound checking) to sophisticated theorem proving (e.g., non-interference).



Ignacio Cascudo
Assistant Research Professor

Ignacio Cascudo received a Ph.D. in Mathematics from the University of Oviedo, Spain, in 2010. After that, he was a postdoctoral researcher at the Centrum Wiskunde en Informatica (CWI) Amsterdam, the Netherlands, and later at the Department of Computer Science of Aarhus University in Denmark. Between 2016 and 2019, he was first assistant professor and then associate professor at the Department of Mathematics of Aalborg University, Denmark. In September 2019, he joined the IMDEA Software Institute as a research assistant professor.

Research Interests

Ignacio's main research interests are within the area of cryptography, specially regarding threshold cryptography technologies such as secret sharing and secure multi-party computation, which study how to distribute information and computations among a number of servers in a privacy-preserving way. He is also interested in applications of these techniques to problems such as random number generation, and in the interplay between these problems and other research fields such as the theory of error-correcting codes, and areas of pure mathematics (algebraic geometry and number theory, finite fields, and algebraic complexity).



Marco Guarnieri
Assistant Research Professor

From June 2019, Marco is an Assistant Research Professor at IMDEA Software Institute, which he joined as a postdoctoral researcher in July 2018. Before that, he worked as a postdoctoral researcher at ETH Zurich, where he also completed a Ph.D. in the Information Security group. He received his bachelor's and master's degrees in computer engineering from Università degli Studi di Bergamo.

Research Interests

Marco's research focuses on the design, analysis, and implementation of practical systems for securely storing and processing sensitive data. To achieve this goal, he combines concepts and techniques from diverse domains, such as databases, logics, probabilistic models, programming languages, and program verification. He applies his research to the analysis of microarchitectural side-channel attacks (and countermeasures), database security, and the enforcement of probabilistic security policies. More generally, he is interested in security and privacy, programming languages, and formal methods.



Pedro López-García
Researcher

Pedro López-García received a MS degree and a Ph.D. in Computer Science from the Technical University of Madrid (UPM), Spain in 1994 and 2000, respectively. On May 28, 2008 he obtained a Tenured Researcher position at the Spanish National Research Council (CSIC) and joined the IMDEA Software Institute. Immediately prior to this position, he held associate and assistant professor positions at UPM and was deputy director of the Artificial Intelligence unit at the Computer Science Department. He has published more than 70 refereed scientific papers, many of them at conferences and journals of high or very high impact. He served as the local principal investigator of the European projects ES_PASS "Embedded Software Product-based ASSurance," and the FP7 FET ENTRa "Whole-Systems Energy Transparency." He has also participated as a researcher in many other international, national, and regional projects.

Research Interests

His areas of interest include energy-aware software development; multi-language analysis, verification, debugging and optimization of non-functional properties, focusing on resources (energy, execution time, user defined), determinism, non-failure, etc.; automatic static

profiling of resources; abstract interpretation; low energy and highly parallel computing in different application domains (internet of things, healthcare, big data, and HPC); resource-aware program synthesis; automatic control of resources in parallel and distributed computing; tree automata; constraint and logic programming.



José Francisco Morales Researcher

Jose F. Morales joined the IMDEA Software Institute as a postdoctoral researcher in November 2011, after receiving his Ph.D. degree in Computer Science from the Technical University of Madrid (UPM), Spain. Previously, he held a teaching assistant position at the Universidad Complutense de Madrid, starting in 2005.

Research Interests

Jose's past work focused on mechanisms for the efficient execution of logic programs: inference of program properties by abstract interpretation, highly-optimizing translation to low-level code using those properties, and the development of abstractions for the specification and automated construction of abstract machines. His current research interests include the design of multiparadigm languages (declarative, imperative) based on a constraint/logic programming kernel; abstract machines, program optimizations, and native code generation; and program analysis, abstract interpretation, and static and dynamic verification.

faculty members on leave of absence



Juan José Moreno-Navarro Research Professor, on leave

Juan José Moreno-Navarro received his Ph.D. degree in Computer Science from the Technical U. of Madrid (UPM), Spain in 1989. He developed a large part of his Ph.D. at RWTH Aachen (Germany). He has been Full Professor at the UPM Computer Science Department since 1996 and joined the IMDEA Software Institute upon its foundation. He served as Deputy Director up to 2008. Currently he is on leave from the Institute. He has published more than 100 papers in international conferences, books, and journals. He has organized, served in program committees, and given invited talks and tutorials in many conferences in the IST field.

He has been actively involved in research and university policy, serving as General Director for University Policies (Ministry of Education, 2009-2012), General Director for Technology Transfer and Enterprise Development (Ministry of Science and Innovation, 2009) and General Director for Planning and Coordination (Ministry of Science and Innovation, 2008-2009). During this period he has been chairman of CNEAI (Spain's Researcher Activity Evaluation Agency), has been involved in the setting up of several research infrastructures, secretary

of the Spanish University Council and of the Spanish Science and Technology Council, and member of the steering board of several foundations (ANECA, UIMP, CENER-Ciemat, Universidad.es, CSIC, ISCIII, IDAE, etc.)

He has been the founding director of SpaRCIM. He has been responsible for the Spanish ICT research program, in charge on International Relations for IST, FP6 IST Committee member, and Spanish National Contact Point for the Spanish Ministry of Education and Science. He also coordinated the Spanish Turing Year and was general chair of the Spanish Conference of Informatics 2013. He is currently an MP in the Regional Government.

Research Interests

His research interests include all aspects related to declarative and rigorous software development technologies. This includes software development techniques, specially specification languages, automatic generation of code (programming from specifications), and software services description. His interests also include the integration of functional and logic programming. He has led the design and implementation of the language BABEL and took part in the activities of the international committee involved in the design of the language Curry. He is also currently involved in scientific policy analysis, bibliometrics, and research impact evaluation and analysis.

postdoctoral researchers



Álvaro García Pérez
Postdoctoral Researcher

Álvaro García Pérez received his Ph.D. in September 2014, from IMDEA Software Institute and Universidad Politécnica de Madrid. During his Ph.D. his work focused on semantics of programming languages and meta-theory of the lambda calculus. From 2014 to 2016, he was a postdoctoral researcher at Reykjavik University under the supervision of Luca Aceto. During this time, he worked in nominal techniques, process algebras and concurrency theory. He joined IMDEA Software Institute again as a postdoctoral researcher in January 2017, where he works in verification of consensus algorithms and blockchain systems.

Research Interests

Álvaro's research interests range over the topics of concurrent and distributed systems and of semantics of programming languages.



Antonio Faonio
Postdoctoral Researcher

Antonio received his Ph.D. degree in Computer Science from Sapienza University of Rome, Italy, where he was advised by Giuseppe Ateniese. From 2014 to 2017 he was a postdoc researcher at Aarhus University, advised by Jesper Buus Nielsen. Starting from 2017, he is a postdoctoral researcher at IMDEA Software Institute where he works with Dario Fiore on cryptography.

Research Interests

Antonio's interest are in both theoretical and applied cryptography. He worked on leakage-resilient and tamper-resilient cryptography, non-malleability and controlled-malleability, re-randomizable cryptosystems and verifiable mixing networks, subversion resilient cryptography, zero-knowledge proofs, and password-based cryptography.



Ignacio Fábregas
Postdoctoral Researcher

Ignacio Fábregas received both his bachelor degree in Mathematics and Ph.D. in Computer Science in Universidad Complutense de Madrid (UCM). In 2017, he joined the IMDEA Software Institute as a post-doctoral researcher, where he works with Aleks Nanevski on the topic of Separation Logics for Concurrency. Before joining IMDEA Software he was a postdoc in Reykjavik University (Iceland), where he worked with Luca Aceto.

Research Interests

His current research interest are concurrency and logics. In particular, he is interested in separation logics, modal logics, category theory for computer science, and process semantics.



Avinash Sudhodanan
Postdoctoral Researcher

Avinash Sudhodanan received his Ph.D. in Information and Communication Technology from University of Trento (Italy). Prior to joining IMDEA Software Institute, he worked as an Early-Stage Researcher at Fondazione Bruno Kessler (Italy) and spent 18 months at SAP Labs France. Avinash received his Bachelors in Computer Science and Engineering and Masters in Cyber Security from Amrita Vishwa Vidyapeetham University, India.

Research Interests

Avinash's research interests primarily lie in the area of automatic detection of security vulnerabilities in web applications. His Ph.D. research led to the discovery of hundreds of serious security vulnerabilities affecting prominent web sites.



Pablo Chico de Guzmán
Postdoctoral Researcher

Pablo completed his Ph.D. at the Technical University of Madrid, Spain. The focus of his dissertation was on parallel computation and advanced compilation techniques in order to allow more declarative programming techniques. His dissertation was completed while researching at the IMDEA Software Institute. After his dissertation, he worked in several worldwide leading companies in the field of cloud computing. In particular, he developed orchestration tools at Docker for three years. Starting in 2017, he is a postdoctoral researcher at the IMDEA Software Institute where he works with César Sánchez on declarative techniques for massive deployments.

Research Interests

Pablo's research interests are cloud computing and the development of declarative and easy to use tools for complex orchestration of distributed systems.



Yuri Meshman
Postdoctoral Researcher

Yuri Meshman obtained an M.Sc. and a Ph.D. at Technion Israel Institute of Technology, as well as a BSc in Mathematics and a BSc in Computer Science. During his BSc, he worked in an IBM Research group as a student software developer. During his Ph.D., he participated in the Fender project, an international research collaboration between Technion, Haifa and ETH, Zurich. Since March 2017, he is a postdoctoral researcher at the IMDEA Software Institute.

Research Interests

Yuri's current research interest are developing and verifying programs for systems with relaxed operational semantics.



Manuel Bravo
Postdoctoral Researcher

Manuel joined the IMDEA Software Institute as a postdoctoral researcher in June 2018. He obtained his Ph.D. in 2018 from the Instituto Superior Técnico of the Universidade de Lisboa in Portugal and the Université Catholique de Louvain in Belgium where he worked with Prof. Luís Rodrigues and Prof. Peter Van Roy. Before that, he obtained his M.Sc. in 2013 from the Instituto Superior Técnico of the Universidade de Lisboa in Portugal and the Royal Institute of Technology in Stockholm, Sweden.

Research Interests

Manuel's research interest is in the design and implementation of distributed systems. Specifically, he is interested in understanding replication and consistency in such systems.

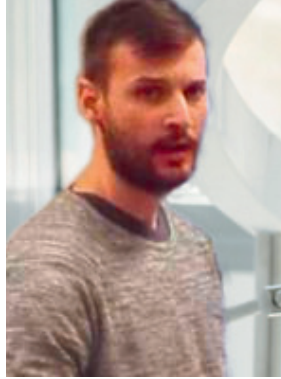


Matteo Campanelli
Postdoctoral Researcher

Matteo obtained his Ph.D. from the City University of New York in 2018 working at the intersection between decision theory, complexity, and cryptography. He was a visiting student at Aarhus University (2016) and at the Stanford Research Institute (2017). He joined IMDEA Software in 2018. Besides cryptographic research he has developed software for Libreoffice and machine learning models for ads quality at Google. He made the mistake of appearing on a few improv comedy stages in NYC; he was never able to surf.

Research Interests

Matteo's current research interests focus on the theory and practice of fast cryptographic protocols in general and on proof systems in particular.



Francesco Gavazzo
Postdoctoral Researcher

Francesco Gavazzo received his BA degree in Philosophy from the University of Padua, his MSc degree in Logic from the Institute for Logic, Language, and Computation (University of Amsterdam), and his PhD in Computer Science and Engineering from the University of Bologna. He joined the IMDEA Software Institute in December 2018.

Research Interests

Francesco's research focuses on programming language theory and formal methods, and specifically on semantics of programming languages. Francesco is currently working on formal techniques for impure higher-order programming languages, as well as for languages for artificial intelligence.

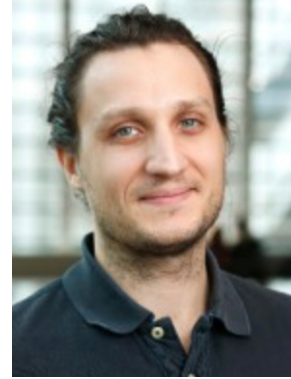


Miguel Ambrona
Postdoctoral Researcher

Miguel Ambrona Castellanos received his Bachelor and Master's degrees in Mathematical Engineering from Universidad Complutense de Madrid. In October 2018, he received his Ph.D. degree in Computer Science from Universidad Politécnica de Madrid and the IMDEA Software Institute under the supervision of Gilles Barthe. After that, he continued working at IMDEA as a postdoctoral researcher, supervised by Dario Fiore and Claudio Soriente. Since June 2019, he is a postdoctoral researcher at NTT Secure Platform Laboratories in Tokyo, under the supervision of Masayuki Abe.

Research Interests

Miguel's research interests include computer-aided cryptography, attribute-based encryption, functional encryption, zero-knowledge proofs and multi-party computation. During his Ph.D., his work focused on the design and implementation of automated tools for analyzing the security of cryptographic constructions.



Matei Istoan
Postdoctoral Researcher

Matei Istoan has a Master's Degree in Computer Science from ENS Lyon and PhD degree from INSA Lyon. Prior to joining IMDEA Software as a Visiting Researcher, he was a Post-doctoral Researcher at Imperial College London. Since October 2019 he is a full time Post-doctoral Researcher at UVSQ Université de Versailles in France.

Research Interests

The research activity of Matei has been focused around circuit architecture, computer arithmetic and signal processing. The context for most of this activity has been reconfigurable circuits, more specifically FPGAs, a topic that has been gathering increasing attention in recent times. In his dissertation, he explored new ways of achieving arithmetic efficiency in computations involving FPGAs, which allow for better performance of the resulting circuits.



Raphaëlle Crubille
Postdoctoral Researcher

Raphaëlle has a Master's degree in Computer Science from the Master Parisien de Recherche en Informatique and a PhD degree from Université Paris 7. She joined IMDEA Software Institute as a postdoctoral research in March 2019.

Research Interests

Raphaëlle's research interests are in probabilistic (higher-order) computation, semantics of programming languages, and metrics for programs.

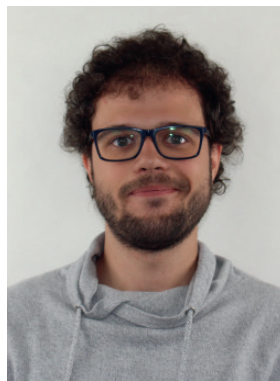


František Farka
Postdoctoral Researcher

František received his Master's degree in Theoretical Computer Science from Charles University, The Czech Republic, and his Ph.D. degree jointly from the University of St Andrews and Heriot-Watt University, UK. In his doctoral work he focused on foundations of constructive proof search with applications to type inference and term synthesis developing proof-relevant semantics of resolution. Starting from November 2018, he worked as a research assistant at Heriot-Watt University on proof-relevant verification of planning languages. He joined IMDEA Software Institute in July 2019. He is working with Aleks Nanevski on verification of shared-memory concurrent programs.

Research Interests

František's research is focused on the application of type theory and logic in the verification of software. He applies concepts arising from these areas to the design of programming languages that facilitate development of software that is correct by construction. More concretely, he has been recently studying separation logic for shared-memory concurrency with particular focus on its algebraic characterisation.



Fernando Macías
Postdoctoral Researcher

Fernando Macías joined the IMDEA Software Institute in September 2019, after a short teaching period at the University of Extremadura, Spain. Before, he carried out his research at the Western Norway University of Applied Sciences and got a PhD in Computer Science from the University of Oslo, Norway in June 2019. Fernando also received an MSc in Computer Science (Ingeniería Informática) in 2013, and a BSc in Computer Science (Ingeniería Técnica Informática) in 2011 at University of Extremadura, where he also worked as a research associate.

Research Interests

Fernando's research focuses on different areas of software engineering, including: Software analysis, testing and verification, including formal methods. Model-driven software engineering, including multilevel modelling, model transformation and model-based reverse engineering of software.



Bishoksan Kafle
Postdoctoral Researcher

Bishoksan received his PhD in Computer Science from Roskilde university, Denmark in 2016. His thesis focused on safety verification of integer programs, using the so called representation of Constrained Horn clauses. During his PhD, he was also a visiting student at NASA Ames Research center, USA. After a post-doc at the university of Melbourne, Australia, he joined the IMDEA Software institute in 2019.

He received a Bachelor degree in Computer Science from Central University of Las Villas, Cuba in 2009 and a joint Master degree in Computational Logic from Dresden University of Technology, Germany; Free university of Bolzano, Italy, and the new university of Lisbon, Portugal in 2012 under an Erasmus Mundus scholarship.

Research Interests

He is interested in automated program analysis and verification. In particular, he applies static analysis, automaton-theoretic approaches, and program specialization techniques to program verification and resource analysis problems based on Horn clauses.

programmers



Anton Trunov

Degree: Engineer – Tomsk State University of Control Systems and Radioelectronics, Russia.



Francy Rodríguez

Degree: Ph.D. – Technical University of Madrid (UPM), Spain.



Mario V. García Roqué

Degree: M.Sc. in Cybersecurity – University Carlos III (UC3M) of Madrid, Spain.



visiting and affiliate faculty



Patrick Cousot
Visiting Faculty

New York University.
Visiting during December 2019.



Gregory Chockler
Visiting Faculty

Royal Holloway University of London.
Visiting during September – December 2019.



Roberto Giacobazzi
Affiliate Faculty



Anindya Banerjee
Affiliate Faculty



Boris Köpf
Affiliate Faculty



research assistants

Research Assistants hold full scholarships or contracts at the Institute, performing research within one of the Institute's research lines under the supervision of a junior or senior researcher, and they undertake their Ph.D. at one of the Universities that the Institute has agreements with. Many of our Research Assistants obtain their degrees from the Technical University of Madrid (UPM), with whom the Institute collaborates in the development of graduate programs.



Maximiliano Klemen
Research Assistant

Degree: B.Sc., Universidad Nacional del Comahue (UNCo), Argentina.

Research: Abstract interpretation-based static analysis for inferring energy consumption information about (concurrent) program executions.



Joaquín Arias
Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Design and implementation of advanced programming languages, including logic programming languages featuring constraints, tabling, and non-monotonic reasoning, and their application to reasoning over stream data and abstract interpretation.



Irfan Ul Haq
Research Assistant

Degree: M.Sc. in Information Technology, National University of Sciences and Technology (NUST), Islamabad, Pakistan.

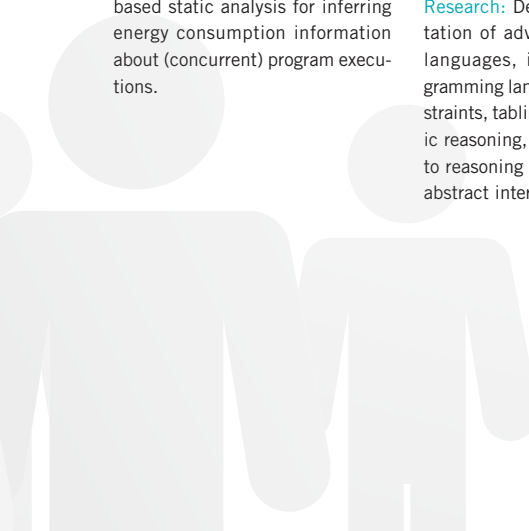
Research: Malware unpacking, binary analysis, web security.



Platon Kotzias
Research Assistant

Degree: M.Sc. in Digital Systems Security, University of Piraeus, Greece.

Research: My research interests lie in malware (detection, analysis, classification) and intrusion detection.





Pablo Cañones
Research Assistant

Degree: M.Sc. in Mathematics for Engineering, Universidad Complutense de Madrid (UCM), Spain.

Research: Information theory applied to obtaining security guarantees for cache algorithms. I focus on modeling the cache architecture, the cache algorithms and the possible side-channel attacks in order to obtain security guarantees of the information leaked.



Paolo Calciati
Research Assistant

Degree: M.Sc. in Informatics, Università della Svizzera Italiana, Lugano, Switzerland.

Research: Improve quality and security of mobile applications using automated testing and malware detection techniques.



Pepe Vila
Research Assistant

Degree: M.Sc. in Computer Engineering, Escuela de Ingeniería y Arquitectura de la Universidad de Zaragoza (EINA), Spain.

Research: Application security with emphasis on client-side web security and side channels. Micro-architectural attacks and countermeasures.



Raúl Alborodo
Research Assistant

Degree: BS in computer Science, Universidad Nacional de Río Cuarto (UNRC), Argentina.

Research: Formal methods applied to concurrent programming, software specification and verification. Design of model-driven methodologies for concurrent programming based on shared resources.



Alejandro Aguirre
Research Assistant

Degree: M.Sc. in Informatics, Université Paris Diderot (Paris 7), France.

Research: Formal methods for software verification, with emphasis on the design and implementation of type systems to check relational properties of programs.



Isabel García
Research Assistant

Degree: M.Sc. in Artificial Intelligence, Technical University of Madrid (UPM), Spain.

Research: Abstract interpretation-based static analysis of programs and how it can be applied to semantic code search. Incremental analysis and verification of programs and its applications. Applications of (constraint) logic programming.



Elena Gutierrez
Research Assistant

Degree: Double BS in Computer Science and Mathematics, Universidad Autónoma de Madrid (UAM), Spain.

Research: Finite and weighted automata theory and applications.



Pedro Valero
Research Assistant

Degree: Double BS in Computer Science and Mathematics, Universidad Autónoma de Madrid (UAM), Spain.

Research: Applications of quasi-orders for solving problems from formal languages and automata theory.



Joakim Öhman
Research Assistant

Degree: M.Sc., University of Gothenburg, Sweden.

Research: Formal verification of software and systems. Design and implementation of type theory, especially for concurrent systems.



Jesús Domínguez
Research Assistant

Degree: M.Sc., National Autonomous University of Mexico, México.

Research: Formal verification of software, concurrency, and type theory.



Felipe Gorostiaga
Research Assistant

Degree: Bsc Universidad Nacional de Rosario (UNR), Argentina.

Research: Lightweight dynamic formal methods, and in particular stream approaches to the runtime verification of reactive systems. The target application is cloud testing and formal monitoring of hybrid and continuous systems.



Anaïs Querol
Research Assistant

Degree: M.Sc. in Computer Science (MPRI), Université Paris Diderot (Paris 7), France.

Research: Design and analysis of cryptographic schemes: zero-knowledge proofs for privacy-enhancing technologies, post-quantum secure protocols, applications of blockchains (cryptocurrencies, electronic voting, healthcare, public accountability...)



Silvia Sebastian
Research Assistant

Degree: M.Sc. in Cybersecurity, Carlos III University of Madrid (UC3M), Spain.

Research: Attribution of malware, lineage of malware, PUP, malware developers in Android systems.



Nikita Zyuzin
Research Assistant

Degree: M.Sc., MPI-SWS / Saarland University, Germany.

Research: Broadly interested in programming languages, type theory, and logic. Immediate interests include secure compilation and reasoning about effectful programs using dependent types.



Daniel Dominguez
Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain.

Research: Mobile security and ecosystem, program and binary analysis of mobile applications, automated reverse engineering, vulnerability detection, metaheuristics for fuzzing techniques.



Kyveli Doveri
Research Assistant

Degree: M.Sc. in Mathematical Logic, Université Paris Diderot, France.

Research: Formal languages of finite and infinite words.



Luis Miguel Danielsson
Research Assistant

Degree: M.Sc. in Software and Systems - Technical University of Madrid (UPM), Spain.

Research: Lightweight formal methods, in particular stream runtime verification of reactive systems. Applied to decentralized systems and systems with other uncertainties such as failures, message losses or message reordering and how to monitor in this context being able to react effectively.



Dimitris Kolonelos
Research Assistant

Degree: M.Sc. in Electrical And Computer Engineering - National Technical University of Athens, Greece.

Research: Design of secure and privacy-preserving cryptographic protocols, zero-knowledge proofs, decentralized protocols, scalability, post-quantum cryptography.



Panagiotis Bougoulas
Research Assistant

Degree: M.Sc. in Electrical and Computer Engineering - National Technical University of Athens, Greece.

Research: Generally interested in programming languages and more specifically program synthesis, functional programming, type systems and automated theorem proving.



Alejandro Naser
Research Assistant

Degree: B.Sc. - Universidad Nacional de Cordoba (UNC), Argentina.

Research: Alejandro's interests lie at the intersection of distributed protocols and formal verification.



Fedor Ryabinin
Research Assistant

Degree: M.Sc. in Computer Science - Université Paris Diderot, France.

Research: Fedor's current research interests are design and implementation of distributed protocols.



Gibran Gómez
Research Assistant

Degree: M.Sc. - Technical University of Madrid (UPM), Spain.

Research: Computer, software and network security. Analysis of blockchains and their use on cybercrime, applying big data and machine learning techniques.



Miętek Bak
Research Assistant

Degree: B.Sc. in Computer Science - Uniwersytet Wrocławski, Poland.

Research: Logical foundations for programming languages, constructive theorem-proving, and proof-theoretic semantics. Intensional analysis of code in total functional programming.

Intern	Period	Nationality
Borja de Regil	10/16-12/19	Spain
Ignacio De Casso	04/18-12/19	Spain
Claudiu Adrian Mihali	07/19-10/19	Romania
Roberto Fernández	09/17-05/19	Spain
Dimitris Kolonelos	09/18-02/19	Greece
Andres Sánchez	09/18-06/19	Spain
Than Hai Tran	10/18-12/19	Vietnam
Fedor Ryabinin	10/18-04/19	Russia
Eva Garcia	10/18-02/19	Spain
Lucas Kuhring	10/18-06/19	Germany
Ankita Sadu	12/18-06/19	India
Soheil Khodayari	01/19-07/19	Iran
Harry Carpio	02/19-06/19	Ecuador
Stevan Coroller	02/19-05/19	France
Srivatsan Lakshmi Narayanan	02/19-05/19	India
Stefano Ottolenghi	02/19-07/19	Italy
Daniel Toniuc	02/19-06/19	Romania
Diego Martinez	07/19-08/19	Spain
Lukas Stasytis	07/19-12/19	Lithuania
David Munuera	09/19-12/19	Spain
Natalia Carpizo	09/19-12/19	Spain
Samuel Garcia	09/19-12/19	Spain
Román Castellarin	09/19-12/19	Spain
Miguel Ángel Sánchez	09/19-12/19	Spain
Mohamed Ali	10/19-12/19	Egypt
Daniel Loscos	10/19-12/19	Spain
Stefan Malewski	11/19-12/19	Chile
Muhammad Laiq	11/19-12/19	India
Mustafa Hafidi	11/19-12/19	Morocco
S.M. Kumail Raza	11/19-12/19	Pakistan



project management

Project management provides additional support for the development of projects and contracts being carried out at the Institute. They are often co-funded by such projects.



Juan José Collazo
Project Manager

Degree: B.Sc. in Economic Sciences, Complutense University, Madrid, Spain.



Teresa Giménez
Project Manager, N-GREENS

Degree: MS in Integrated Systems Management, University of the Balearic Islands, Spain.



Aiora Garalde
Project Assistant

Degree: BS in Business Administration and Management - University of Alicante, Spain; National University of Distance Education, Spain.

IMDEA common services



Begoña Moreno
IMDEA Institutes' Coordinator

Degree: Ph.D. in Economic Science, Universidad de Alcalá, Madrid, Spain.

technical support and infrastructures

Research Support Technical Staff provide support for the research infrastructures provided to the researchers at the Institute. These include virtualization environments, version control systems, research collaboration tools, continuous integration platforms, experimentation harnesses, computing farms, communications, etc. They are currently co-funded by different projects and agreements.



Roberto Lumbreras
**Computing and Communication
Infrastructures**

Degree: M.Sc. Elec. & Computer Eng., Technical University of Madrid (UPM), Spain.



Juan Céspedes
Network and Systems Engineer

Degree: M.Sc. Elec. & Computer Eng., Technical University of Madrid (UPM), Spain.



Gabriel Trujillo
**Systems Administrator
(until May 2019)**

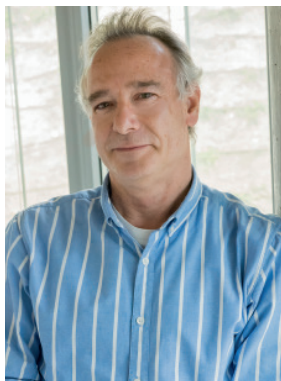
Degree: AD in Network Systems Administration, El Rincón, Las Palmas, Spain.



Tomas Kriukelis
**Systems Administrator
(since September 2019)**

Degree: M.Sc. in Telecommunications - European University of Madrid, Spain.

REDIMadrid



Carlos Ricardo de Higes
REDIMadrid Technician and
Computer Operations

Degree: Licensed Electrical Technician, Instituto Juan de la Cierva, Madrid, Spain.



David Rincón
REDIMadrid Network Engineer

Degree: B.Sc. in Telecommunications, Technical University of Valladolid, Spain.



Oscar Rebollo
REDIMadrid Network Engineer

Degree: M.Sc. in Technical Telecom Engineer - Technical University of Madrid (UPM), Spain.

management & administration



María Alcaraz
General Manager

Degree: PADIIT – IESE (2019), MBA – Escuela Internacional de Negocios, CEREM, Madrid, Spain.



Tania Rodríguez
General services coordinator

Degree: M.Sc. in Business Administration, Universidad Centroamericana José Simeón Cañas.



Carlota Gil
Accounting & Tax Officer

Degree: M.Sc. in Business Administration, Universidad Rey Juan Carlos, Madrid, Spain.



Lídice González
Administrative Assistant

Degree: BD in Education - University of Pedagogical Sciences Félix Varela, Cuba.



Andrea Iannetta
Human Resources Assistant

Degree: B.Sc. in Economics, Godspell College, Argentina.



Ignacio Echaide
Human Resources Coordinator

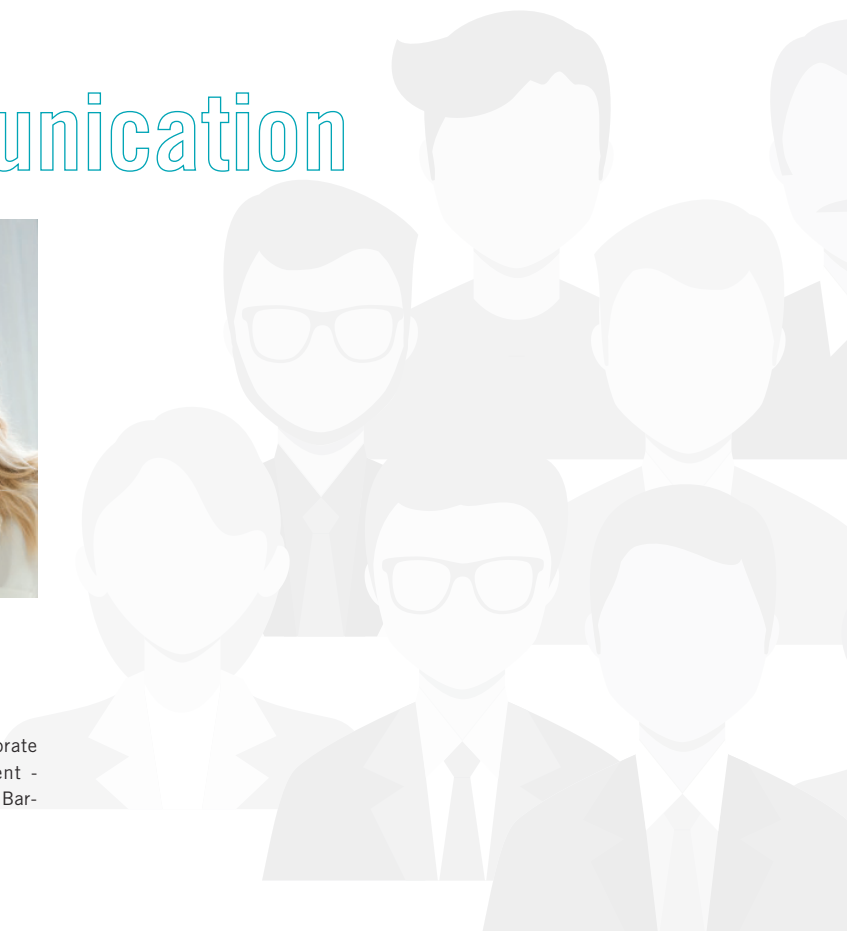
Degree: M.A. in Law - Autonomous University of Madrid (UPM), Spain.

communication



Blanca Gutiérrez
Communication Manager

Degree: M.Sc. MS in Corporate Communication Management - EAE, OBS and University of Barcelona, Spain.





research projects and contracts

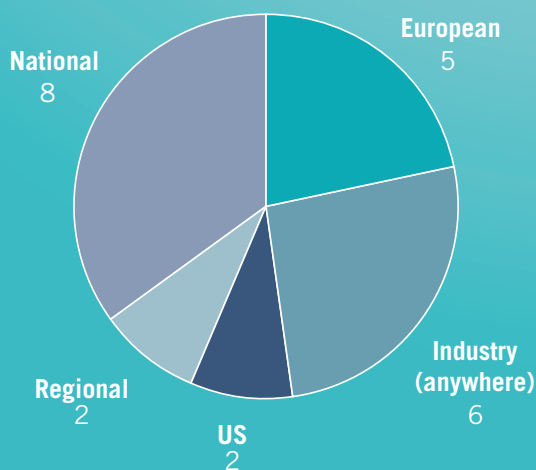


Figure 1. Projects by origin of funding

An important source of funding and technology transfer opportunities for the Institute are projects, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. During 2019, the Institute participated in a total of 23 funded research projects and contracts, of which more than one half (13, or almost 57%) involve collaboration with industry and five of them have direct industrial funding. Of these 23 projects, 13 come from international sources (5 funded by the European Union, 2 by the ONR-US agency, and 4 by foreign companies), 10 have a national source, and funds for 2 come from regional sources, either through competitive calls or via contracts with companies. Figure 1 shows the origin of project funding. In the same year, the Institute benefited from 15 fellowships.

The trend of external funding for the period 2012-2019 is shown in Figure 2. The amount of external funding for 2019 amounts to €2.1M, with the percentage of external funding for research and innovation w.r.t. the total Institute budget reaching 40%.

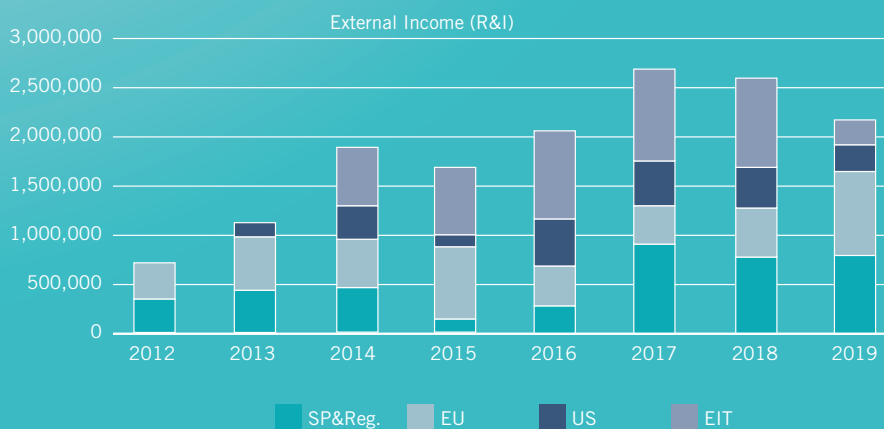


Figure 2. Evolution in external funding since 2012

Projects Running in 2019

SynCrypt

Automated Synthesis of Cryptographic Constructions

Funding: US Office of Naval Research (ONR), through Stanford University

Duration: 2015-2019

Project Coordinator: Res. Prof. Gilles Barthe

SynCrypt is a joint project with Stanford University, University of Pennsylvania, and SRI, funded by ONR and which runs from September 2015 until March 2019. SynCrypt is the continuation of AutoCrypt project and the budget allocated for IMDEA Software is over 1 Million Euros. SynCrypt aims to develop synthesis techniques and tools for cryptographic constructions, and for cryptographic implementations. Building on their previous work, IMDEA researchers will develop synthesis tools for generating, transforming, and hardening cryptographic constructions.

Within the project, the IMDEA Software team plans to extend their EasyCrypt tool (<http://www.easycrypt.info>) to handle proof generation for lattice-based systems. This will require a fair amount of enhancements to EasyCrypt. IMDEA will extend the logical rules for proving security of cryptosystems to reason about noise growth and will apply these tools to analyze lattice-based identity-based systems and attribute-based encryption schemes.



HACrypt

High-Assurance Cryptography

Funding: US Office of Naval Research (ONR), through Stanford University

Duration: 2019-2022

Project Coordinator: Res. Prof. Gilles Barthe

HACrypt is the continuation of SynCrypt project. HACrypt is a collaborative project coordinated by Stanford University, with the participation of the University of Pennsylvania, and Johns Hopkins University, funded by ONR and which runs from June 2019 until June 2022. The budget allocated for IMDEA Software in HACrypt projects is over 600 K Euros. The project will contribute to the emergence of high-assurance cryptography through the design and security analysis of key components for a high-assurance cryptographic toolbox (in particular, RNGs, proof systems). In addition, this project will develop new tools and methods for building high-assurance cryptographic implementations. The HACrypt project build on the results developed in its predecessors, Autocrypt and SynCrypt projects.

Within the project, the IMDEA Software team will work in the following research topics: automated generation of high-assurance advanced cryptographic implementation, high assurance of correctness and security against side-channel attacks and automated synthesis of cryptographic constructions



EIT Digital Spain

EIT Digital Spain: Coordination and Joint Activities



Funding: Spanish Ministry of Economy, Industry, and Competitiveness

Duration: 2018-2020

Principal Investigator: Assoc. Res. Prof. Juan Caballero

This project continues the action of its predecessor granted in 2015 and aims to boost the activities of the Spanish node of EIT Digital. The duties of IMDEA Software, as project beneficiary, focus on contributing to the progress of the network in collaboration with the members of the node with a twofold objective: on the one hand, to improve knowledge of the KIC possibilities in order to take maximal profit from the innovation program, and on the other hand to spread the activities of the KIC in the National ICT sector at all levels: large companies, SMEs, entrepreneurs, students, academia and researchers.

BLOQUES-CM

Contratos inteligentes y blockchains escalables y seguros mediante verificación y análisis

Funding: Regional Government of Madrid

Duration: 2019–2022

Project Coordinator: Assoc. Res. Prof. Juan Caballero

The BLOQUES-CM project addresses the growing importance of blockchain-based technology, which, by using techniques from distributed systems and cryptography, and within the framework of a distributed database that registers transactions, allows participants to agree on which of these transactions are valid. Once transactions are accepted, the blockchain ensures that these cannot be modified. Likewise, it is practically impossible to present as valid a non-existent transaction.

In particular, BLOQUES-CM will advance the state of the art in: anonymity and integrity properties of distributed ledgers; verification of infrastructures for distributed ledgers; proofs of correction and resource usage of smart contracts; the application of testing to distributed ledgers; and the availability and development of tools to support the previous goals.

BLOQUES-CM is a consortium involving groups from Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and the IMDEA Software Institute, which is the project coordinator.



MadridFlightOnChip

Consortium Madrid for Next-Generation Flight Systems Based on Multiprocessor *System-on-a-Chip* Technology

Funding: Regional Government of Madrid

Duration: 2019–2021

Principal Investigators: Assoc. Res. Prof. César Sánchez – Asst. Res. Prof. Alessandra Gorla

Madrid Flight on Chip (MFoC) is a research and innovation project linked to the RIS3 Smart Specialization Platform and co-funded by the Comunidad de Madrid. It consists on a platform for the development of space missions, particularly research and demonstrator satellites. IMDEA Software will focus on developing innovation in the area of software validation, specifically adapted to these missions.

MFoC is a consortium involving groups from academic partners, Universidad Carlos III de Madrid and IMDEA Software, and also from the industrial partners CENTUM Solutions, GENERA Soluciones Tecnológicas, Knowledge Centric Solutions, MARM Desarrollo de Sistemas, and SENER Aeroespacial, which is the project coordinator.

e-TUR2020

e-TUR2020. Turismo & Retail

Funding: Spanish Ministry of Economy, Industry, and Competitiveness – CDTI

Duration: 2015-2020

Principal Investigator: Assoc. Res. Prof. Juan Caballero

e-TUR2020 is a 4-year Spanish joint industrial research project funded by the Centre for the Development of Industrial Technology (CDTI). The aim of e-TUR2020 is to create a new on-line platform for the tourism sector that will enrich the sector's mobile applications with new services for tourists, tourist sector agents, and companies from other sectors. The e-TUR2020 project involves 6 industrial partners (Compartia, Eureka, Groupalia, SoluSoft, Tecnom, Zemsania). The industrial partners subcontract parts of the work to 4 research and development centers (Eurecat, IMDEA Software Institute, PCT, and Universidad Carlos III de Madrid). Within e-TUR2020, the IMDEA Software Institute will manage the security aspects. To this end, the Institute will contribute to research and develop techniques to secure the information exchange.



TRACES

Technologies and tools for Resource-Aware, Correct, Efficient Software



Funding: Spanish Ministry of Economy, Industry, and Competitiveness

Duration: 2016-2020

Principal Investigators: Assoc. Res. Prof. Manuel Carro – Res. Prof. Manuel Hermenegildo

The TRACES project revolves around the need of change in the fundamental tools and approaches which underlie the software engineering techniques to be applied in the very near future. For this purpose TRACES includes three main research lines: 1) Resource-aware computing: being able to determine safe (and maybe approximate) bounds for the resource consumption of software in a given hardware, and optimize it as much as possible, is necessary to ensure the correctness of embedded devices in terms which are more general than just functional correctness; 2) Advanced techniques to ensure functional correctness: these include not only infinite-state verification, but also debugging, synthesis of concurrent software, probabilistic / heuristic methods, and lean methods, such as testing and runtime / dynamic verification. These are necessary when, for example, the boundaries of a computer system are not well-known in advance, or the interactions with the outside world can only be probabilistically modeled; 3) New language technologies: new environments, tasks, and missions make it necessary to adapt existing languages to them or to create languages anew. Contrary to widespread belief, new languages and programming models are constantly created not only in academia but also in industry with the aim of either taking advantage of new devices or of performing tasks (e.g., knowledge-related) which would be too complex to write (and to ensure correct!) in traditional languages.

BOSCO

Foundations for the development, analysis and understanding of BLock chains and Smart COntracts



Funding: Spanish Ministry of Science, Innovation and Universities

Duration: 2019-2021

Principal Investigators: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Pierre Ganty

The main goal of BOSCO project is the development of foundations for (1) the formal analysis of the distributed infrastructure that implements Blockchains and how to optimize its performance; and (2) the analysis and verification of smart contracts. Proving mathematically the correctness of software is not a new problem and many aspects has been extensively studied for years. However, Blockchains present new risks and opportunities.

In terms of the infrastructure, there are two fundamental elements in the Blockchain: cryptographic functions and consensus algorithms to reconcile the distributed database. One of the lines of this project is devoted to the study how to verify consensus algorithms, which is critical to guarantee that the Blockchain does not

present errors that could be exploited. Another line in this project is devoted to hardware based optimizations, and another task studies how to improve the scalability of consensus using sharding.

In addition, the most promising applications of Blockchain will be the use of smart contracts. On one hand, smart contracts are a computer representation of legal contracts among entities, possibly humans. On the other hand, smart contracts are very similar to computer programs in the sense that they precisely describe the steps taken in the evolution of a contract and what are the capabilities of each agent at each point. From this second point of view, smart contracts are pieces of software, with the same potential and risks of pitfalls. Technically, smart contracts present some of the opportunities because some of the aspects that make software verification hard are not present, like complex computer architectures, dynamic memory and instruction level parallelism. On the other hand, to reason about smart contracts we need to model aspects like interactions between agents and the interleavings between different accesses to the Blockchain. We devote two lines to develop the foundations for the study of smart contracts. Particularly, one of the lines study the deductive verification using interactive theorem provers. The other focuses on logics for the specification and runtime verification.

SCUM

Securing Untrusted Machines



Funding: Spanish Ministry of Science, Innovation and Universities

Duration: 2019-2022

Principal Investigators: Assoc. Res. Prof. Juan Caballero – Assoc. Res. Prof. Dario Fiore

The objective of the SCUM project is increasing the trust on the machines used to build information systems. The project focuses on three fundamental challenges related to this objective: (1) Providing trust on remote computations and data storage on third-party machines; (2) Detecting systems that may have been compromised, and thus should not be trusted, as well as identifying those responsible for the compromise; and (3) Removing vulnerabilities in the software and platform components used as building blocks of the digital systems.

The work plan of the project is organized in 3 research lines covering those challenges: Untrusted Third-Party Machines, Untrusted Compromised Systems and Untrusted Vendors.

The research carried out in SCUM will impact multiple booming digital economy markets including data protection, cloud computing, blockchain, malware defenses, and secure software testing. To achieve its objectives the scientific team of the SCUM project comprises researchers from one of Europe's leading research groups in cybersecurity, as well as Ph.D. students and prominent international collaborators.

AxE Javascript

Auditable E-voting using Javascript

Funding: Spanish Ministry of Economy, Industry, and Competitiveness and European Regional Development Fund

Duration: 2016-2019

Principal Investigator: Res. Prof. Gilles Barthe

The AxE Javascript Project aims to bring a solution to confidence problems in the field of security in electronic voting systems through the development of e-voting software with the highest possible correctness and security properties. Identifying and defining properties for security in e-voting systems and developing and implementing new methods providing real evidence of correctness and security in e-voting systems, AxE Javascript project aims to develop a solution for e-voting including the highest actually possible guarantees regarding code correctness and security. This will allow a significant improvement in the transparency of e-voting systems used by electoral organizations.



DataMantium

Secure Cloud Computation and Communication for Hostile Environments

Funding: Spanish Ministry of Economy, Industry, and Competitiveness and European Regional Development Fund

Duration: 2016-2019

Principal Investigators: Assoc. Res. Prof. Dario Fiore – Res. Carmela Troncoso

The goal of DataMantium project is to develop security mechanisms to protect the integrity and privacy in users data and processes in untrusted cloud scenarios. The results of the project totally aim at issues specially relevant in cybersecurity and digital trust, such as cryptography, to protect the information's confidentiality and integrity and the development of communication technologies in private and secure networks.



Europa Excelencia

CRYPTOEPIC: Criptografía para asegurar la privacidad y la integridad de la computación en máquinas no confiables

Funding: Spanish Ministry of Economy, Industry, and Competitiveness

Duration: 2018-2021

Principal Investigator: Assoc. Res. Prof. Dario Fiore

The *Europa Excelencia* grants, funded by the MINECO, support proposals submitted to ERC Starting and Consolidator Grants from Spanish research centers which were ranked with A, but not funded due to budget constraints. IMDEA Software has obtained two of these grants to support the development of some tasks included in the research proposals submitted to the European Research Council (for Consolidator Grants and Starting Grants, both by Dario Fiore) in the 2017 and 2018 calls.



RACCOON

A Rigorous Approach to Consistency in Cloud Databases

Funding: European Union, European Research Council – H2020 Framework Program

Duration: 2017-2021

Principal Investigator: Assoc. Res. Prof. Alexey Gotsman



The goal of this project is to develop a synergy of novel reasoning methods, static analysis tools, and database implementation techniques that maximally exploit parallelism inside cloud databases, while enabling application programmers to ensure correctness. We intend to achieve this by first developing methods for reasoning formally about how weakening the consistency guarantees provided by cloud databases affects application correctness and the parallelism allowed inside the databases. This will build on techniques from the areas of programming languages and software verification. The resulting theory will then serve as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that its side effects do not compromise application correctness.

Mathador

Type and Proof Structures for Concurrent Software Verification

Funding: European Union, European Research Council – H2020 Framework Program

Duration: 2017-2022

Principal Investigator: Assoc. Res. Prof. Aleksandar Nanevski



The grand challenge of this project is to remove existing limitations which make proofs generated with proof assistants unmanageable by humans, and to scale dependent types to support the implementation of stateful concurrent programs and their correctness proofs simultaneously. By applying the modularizing power of dependent types to both programs and proofs, the project will obtain novel and scalable foundations for the field of concurrent software verification. Writing mechanized proofs of software, concurrent or otherwise, is generally considered infeasible. But if one chooses the right linguistic abstractions to express the proofs, we argue that it does not have to be so. This observation is supported by our encouraging preliminary results. The project will design further novel linguistic abstractions that facilitate engineering of practically feasible formal proofs, and experimentally evaluate them by mechanically verifying extensive concurrent programs drawn from realistic applications, such as concurrent garbage collectors, OS kernels, and popular open-source concurrent libraries.

ELASTEST

ElasTest: an Elastic Platform for Testing Complex Distributed Large Software Systems

Funding: European Union – H2020 Framework Program

Duration: 2017-2019

Principal Investigators: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Juan Caballero



This project aims at significantly improving the efficiency and effectiveness of the testing process and, with it, the overall quality of large software systems. For this, we propose to apply the “divide-and-conquer” principle, which is commonly used for architecting complex software, to testing by developing a novel test orchestration theory and toolbox enabling the creation of complex test suites as the composition of simple testing units. This test orchestration mechanism is complemented with a number of tools that include: (1) Capabilities for the instrumentation of the Software under Test enabling to reproduce real-world operational conditions thanks to features such as Packet Loss as a Service, Network Latency as a Service, Failure as a Service, etc.; (2) Reusable testing services solving common testing problems including Browser Automation as a Service, Sensor Emulator as a Service, Monitoring as a Service, Security Check as a Service, Log Ingestion and Analysis as a Service, Cost Modeling as a Service, etc; (3) Cognitive computing and machine learning mechanisms suitable for ingesting large amounts of knowledge (e.g. specifications, logs, software engineering documents, etc.) and capable of using it for generating testing recommendations and answering natural language questions about the testing process. The ElasTest platform thus created shall be released basing on a flexible Free Open Source Software and a community of users, stakeholders and contributors shall be grown around it with the objective of transforming ElasTest into a worldwide reference in the area of large software systems testing and of guaranteeing the long term sustainability of the project generated results.

OPENQKD

Open European Quantum Key Distribution Testbed

Funding: European Union – H2020 Framework Program

Duration: 2019-2022

Principal Investigator: Assoc. Res. Prof. César Sánchez



The Project goal is the establishment of QKD-based secure communications as a well-accepted, robust and reliable technology instrumental for securing traditional industries and vertical application sectors, and to prepare the deployment of a future Europe-wide QKD-based infrastructure.

The high level objectives are: raising the awareness about the maturity of QKD; working with end-users to test and validate end-to-end security for businesses and industry sectors based on or requiring QKD; advancing QKD systems and QKD-based secure-communication solutions to meet market demands in terms of specifications, standards, and certification; and, finally, provide several open test facilities to encourage the development of new QKD-based applications by a wide community.

The consortium is composed by 38 members (including 18 private European companies), 4 of them from Spain. The IMDEA Software Institute participates by providing the REDIMadrid telecommunications network, managed by the Institute, as physical infrastructure, as well as the expertise of the REDIMadrid staff. With this participation, a research network will be deployed over the existing REDIMadrid. That makes it possible to work around renting network capacity, which is less flexible than the dark fiber whose rights of use were already bought by IMDEA Software: in the REDIMadrid network, quantum transmission channels will physically coexist with traditional (research) channels without interfering, thereby making it possible to verify how the proposed quantum distribution solutions work in a real environment.

ACCORD

Accelerated Ordering Service for Distributed Ledgers

Funding: European Union, Marie Curie Action (Individual Fellowship) – H2020 Framework Program

Duration: 2019-2021

Principal Investigator: Asst. Res. Prof. Zsolt István



The ACCORD project aims to increase distributed ledger throughput by at least an order of magnitude, while lowering latencies by a similar factor. To achieve this, the project focuses on the core component of DL systems, namely, distributed consensus, that is used to establish an absolute order of transactions. This ordering operation (service) is typically the main performance bottleneck in DLs. To fully exploit emerging network technologies and to overcome stagnating CPU performance, ACCORD will use hardware acceleration (i.e., FPGAs) to offload the steps required by the ordering service. The outcome of this project is a DL design with performance that allows it to be deployed in use-cases in which DLs are inadequate today (e.g., trading).

POST

POST: Novel Constructions of Proof-of-Spacetime

Funding: Protocol Labs

Duration: 2018-2020

Principal Investigators: Assoc. Res. Prof. Dario Fiore – Post. Res. Matteo Campanelli



Protocol Labs

Proofs of Space Time (PoST) allow a user to show she has been storing a file for a certain amount of time. They are an important building block of the FileCoin protocol. Current constructions for PoST are based on the following paradigm: iterate a Proof of Replication (PoRep) and prove that all the repetitions are correct through a SNARK system. Unfortunately, applying even a state-of-the-art general purpose SNARK would result in PoST with impractical performances on the prover's side. The goal of this project is to design new PoST developing new SNARKs that are especially tailored to Proofs of Replication and their iteration.

INTEL

Information Flow Tracking across the Hardware-Software Boundary

Funding: Intel Corporation

Duration: 2018-2021

Principal Investigators: Asst. Res. Prof. Marco Guarnieri.

This project focuses on the development of a novel, principled approach for software defenses against SPECTRE-style attacks. Its key feature is that it is backed by semantic security guarantees, yet it does not require programmers to provide any specification or annotations. It will pave the way to formally characterize the security guarantees envisioned by the project; these will lead to a blueprint for the design, implementation, and evaluation of program analysis techniques to detect this kind of attacks. The project is completely funded by Intel, and puts together a team from the IMDEA Software Institute, the University of Saarland, KU Leuven, and the Technical University of Graz,



NEC Industrial Research Grant

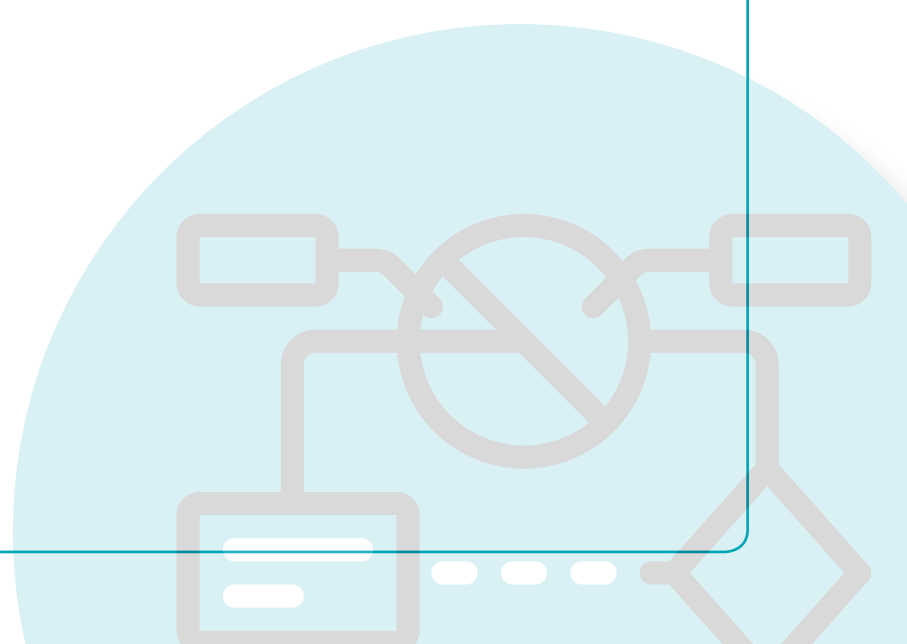
Secure Cloud Storage with Controlled Computation

Funding: NEC

Duration: 2018-2019

Principal Investigator: Assoc. Res. Prof. Dario Fiore

IMDEA researchers have started a research program funded by NEC to investigate in two major directions. On the one side, they plan to devise cryptographic schemes that reconcile user privacy with the great computational power of cloud providers that is key in computations over large data sets. On the other hand, they will investigate what benefits can secure hardware provide in this context and how secure hardware can improve the provisions of cryptographic protocols for cloud storage.



Some companies with which the IMDEA Software Institute has collaborated through projects and contracts to date

Project/Contract	Funding Entity	Industrial Partners
MOBIUS	FP6: IP	France Telecom, SAP AG, Trusted Labs
HATS	PF7: IP	Fredhopper
NESSoS	PF7: NoE	Siemens, ATOS
ES_PASS(<i>Through an associated group at UPM.</i>)	ITEA2, MITyC	Airbus France, Thales Avionics, CS Systèmes d'Information, Daimler AG, PSA Peugeot Citroen, Continental, Siemens VDO Automotive, EADS Astrium, GTD, Thales Transportation, and IFB Berlin
EzWeb	MITyC	Telefónica I+D, Alimerka, Integrasys, Codesyntax, TreeLogic, Intercom Factory, GESIMDE, Yaco, SoftTelecom
DESAFIOS-10	MICINN	BBVA-GlobalNet, LambdaStream, Deimos Space
PROMETIDOS	Madrid Regional Government	Deimos Space, Atos Origin, BBVA-GlobalNet, Thales, Telefónica I+D
MTECTEST	Madrid Regional Government	Deimos Space
SEIF awards	Microsoft SEIF	Microsoft Research
Ph.D. Scholarships	Microsoft	Microsoft Research
ENTRA	FP7: STREP	XMOS
VARIÉS	FP7: ARTEMIS	Barco NV, HI iberia, IntegraSys, Tecnalía, Sirris, Spicer, Fraunhofer Gesellschaft, Pure-Systems GmbH, Stiftelsen Sintef, Autronica, Franders Mechatronics Technology Centre, Atego Systems, Teknologia Tutkimuskeskus VTT, Mobisoft, HIQ Finland, Softkinetic Sensors, Macq, Metso Automation.
4CaaST	FP7: IP	Telefónica I+D, SAP, France Telecom, Telecom Italia, Ericsson, Nokia-Siemens, Bull SAS, 2nd Quadrant, Flexiant
POLCA	FP7: STReP	Maxeler, Recore
Cadence	EIT	Reply SpA
FI-PPP-Liaison	EIT	Engineering Ingegneria Informatica SpA, Orange, Thales, Create-Net
NEXTLEAP	H2020	Merlinux
ELASTEST	H2020	Fraunhofer, Telecom Italia, Atos, Tikal Technologies, IBM Ireland, Relational
DataMantium	MINECO	ScytI
AxE Javascript	MINECO	ScytI
HC@WORKS	EIT	Atos, Thales, Engineering, CEA List
SMAPPER	EIT	Telecom Italia, Backes SRT
ANTIFRAUD	EIT	Reply SpA
MadridFlightOnChip	Madrid Regional Government	SENER Aeroespacial, CENTUM, GENERA, REUSE, MARM
Information Flow Tracking across the Hardware-Software Boundary	Intel Corporation	Intel Corporation
POST	Protocol Labs	Protocol Labs
Contracts	Microsoft	Microsoft Research
Contracts	AbsInt	AbsInt GmbH
Contracts	Boeing	Boeing Research & Technology Europe
Contracts	Telefónica	Telefónica I+D
Contracts	LogicBlox	LogicBlox
Contracts (eTUR2020)	Zemania	Zemania, Tecnomcom, Groupalia, Solusoft, Eurona, BDigital
Contracts	NEC	NEC Laboratories Europe GmbH
Contracts	INDRA	INDRA Sistemas S.A.
Contracts (Ciber 4.0)	RedBorder	RedBorder.
Contracts (RiskIoT)	Nextel	Nextel S.A. Ingeniería y Consultoría
OPENQKD	H2020	Services Industriels de Geneve, Toshiba Research Europe, Id Quantique, Deutsche Telekom, Rohde and Schwarz Cybersecurity, ADVA Optical, Mellanox, Nokia Bell Labs, Fragmentix, Telefónica I+D, British Telecom, Orange, Citycom, DIN Deutsches Institut für Normung, NPL Management, Thales, IXBLUE, Thales, MT Pelerini Group SA
ACCORD	H2020	IBM Research
AutoCrypt	ONR - Stanford University	SRI International
SynCrypt	ONR - Stanford University	SRI International
Contracts (BBVA)	BBVA	BBVA
Contracts	GMV	GMV

fellowships

1. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2018 and ending in 2023 (**Pierre Ganty**).
2. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2016 and ending in 2021 (**Alexey Gotsman**).
3. *Estabilización Doctores I3 grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2017 and ending in 2019 (**Aleks Nanevski**).
4. *Juan de la Cierva grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2022 (**Manuel Barvo**).
5. *Juan de la Cierva grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2022 (**Zsolt István**).
6. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2023 (**Marco Guarnieri**).
7. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2023 (**Manuel Bravo**).
8. *Atracción de talento grant*, Madrid Regional Government, awarded in 2019, and ending in 2024 (**Niki Vazou**).
9. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2017 and ending in 2021 (**Elena Gutiérrez**).
10. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture, and Sports, awarded in 2017 and ending in 2021 (**Isabel García**).
11. *FPU Doctoral Grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2023 (**Silvia Sebastián**).
12. *FPU Doctoral Grant*, Spanish Ministry of Science, Innovation, and Universities, awarded in 2019 and ending in 2024 (**Luís Miguel Danielsson**).
13. *FGJ Doctoral Grant*, Madrid Regional Government, awarded in 2019 and ending in 2019 (**Silvia Sebastián**).
14. *Predoctoral Grant*, Protocol Labs, awarded in 2019 and ending in 2020 (**Dimitris Kolonelos**).
15. *La Caixa Doctoral Grant*, La Caixa Foundation, awarded in 2018 and ending in 2021 (**Anaïs Querol**).



Projects to Start in 2020

TEZOS

TEZOS collaboration multi-annual research, training, and dissemination program



Funding: TEZOS Foundation

Duration: 2020–2025

Principal Investigators: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Manuel Carro

The IMDEA Software Institute and the Tezos Foundation are finishing a framework agreement to further maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation, through the French company Nomadic Labs, is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem. To that end, the projects to be granted under this agreement will greatly contribute to the research, development, and long-term success of Tezos.

IMDEA's program will focus on the technology surrounding the Tezos cryptographic ledger and smart contracts, which will help advance developments in privacy, correctness, robustness, and scalability.

BBVA

Research agreement with BBVA



Funding: BBVA

Duration: 2020

Principal Investigators: Assoc. Res. Prof. Dario Fiore – Post. Res. Antonio Faonio

Thanks to this agreement BBVA and the IMDEA Software Institute will explore the application of cryptographic techniques in the financial sector - techniques that make it possible for data to be shared and analyzed without exposing their content to third parties thanks to algorithms, protocols and encryption systems. Among various privacy-enhancing technologies, zero knowledge proofs (ZKP) is one that has the greatest potential, and it will be the main subject of this new team's study. This technology uses cryptographic algorithms to make it easier to verify the accuracy of information, without having to share the data that comprise it. This way, it can help create data-based solutions in which customers' sensitive data is not exposed to third parties (as it is not necessary to share the data with them to prove that they are accurate). The goal is for the research to translate into tangible advances that make it possible to transfer the benefits of this technology to the financial sector, the corporate world, the scientific community and society as a whole.

SECURITAS

Red de Investigación en Ciberseguridad y Privacidad

Funding: Spanish Ministry of Economy, Industry, and Competitiveness

Duration: 2020-2022

Principal Investigator: Assoc. Res. Prof. Dario Fiore

The Research Network on Cybersecurity and Privacy (SECURITAS), which is coordinated by Rovira and Virgili University and includes researchers from 9 spanish universities and research centers, aims at consolidating and reinforcing a common area of research in cybersecurity and high-level information privacy in Spain. The various groups are working to formalize an alliance to make research and its transfer more effective and competitive. In order to do this, each of the groups will contribute their experience in one or more specific aspects so that multifarious research advances become possible through cooperation with the rest of the members of the network. At the same time, the network will work so that the developed solutions are effectively transferred to society through the work of a valorization expert, who will be an intermediary between universities and the interested productive sectors. Another objective of the network will be to promote the participation of different groups in national and European initiatives, specifically in the H2020 and Horizon Europe programs of the European Commission. The experience of the groups that are currently participating in European projects will help the rest of the groups to explore the possibilities of participating in proposals with another member of the network or on their own.



Universitat
de les Illes Balears



UNIVERSITAT ROVIRA I VIRGILI



Universidad
de La Laguna



Universitat Oberta
de Catalunya



Universitat Autònoma
de Barcelona



UNIVERSIDAD
DE MÁLAGA



Universitat de Lleida



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH



Universitat
Pompeu Fabra
Barcelona

MOKA

Moka: Improving App Testing with Automated Mocking

Funding: FACEBOOK

Duration: 2020

Principal Investigator: Asst. Res. Prof. Alessandra Gorla

The project includes research groups from Georgia Institute of Technology, University of Minnesota and IMDEA Software. The goal of this project is to improve app testing by allowing, supporting, and partially automating the generation of smart test mocks. Specifically, it will develop and implement MOKA, a family of techniques that developers can use to collect, generalize, and use test mocks for manually and automatically generated tests. Intuitively, given an app under test (AUT), these techniques will (1) use record-and-reply techniques to collect mock data from the interactions between the AUT and the software environment, (2) generalize the collected data into smart test mocks, and (3) use these mocks to generate new tests. If successful, this research will provide unprecedented advantages to developers, who will be able to perform a more effective automated app testing while also mitigating the problem of test flakiness.





communication and dissemination

communication
and dissemination







Publications

The vast majority of the research of the Institute is published at highly-ranked conferences and journals. In line with what is common in Computer Science, and unlike what happens in other disciplines, conferences are often preferred to journals for a variety of reasons. Therefore, most of our researchers target them primarily to present bleeding-edge work, and submit to journals only archival papers after they have been presented at the leading conferences of their fields.

In addition to peer-reviewed papers, we list in this section conference proceedings edited by our researchers, articles in books, and theses (at the levels of Bachelor, Master, and PhD).

Refereed Publications

Journals

1. Gilles Barthe, Thomas Espitau, Justin Hsu, Tetsuya Sato, Pierre-Yves Strub. *Relational -Liftings for Differential Privacy*. Logical Methods in Computer Science, Vol. 15, Num. 4, December 2019.
2. Patrick Baillot, Gilles Barthe, Ugo Dal Lago. *Implicit Computational Complexity of Subrecursive Definitions and Applications to Cryptographic Proofs*. Journal of Automated Reasoning, Vol. 63, Num. 4, pages 813–855, December 2019.
3. Alejandro Calleja, Juan Tapiador, Juan Caballero. *The MalSource Dataset: Quantifying Complexity and Code Reuse in Malware Development*. IEEE Transactions on Information Forensics and Security, Vol. 14, Num. 12, pages 3175–3190, IEEE, December 2019.
4. César Sánchez, Gerardo Schneider, Wolfgang Ahrendt, Ezio Bartocci, Domenico Bianculli, Christian Colombo, Yliès Falcone, Adrian Francalanza, Srdan Krstic, João M. Lourenço, Dejan Nickovic, Gordon J. Pace, José Rufino, Julien Signoles, Dmitriy Traytel, Alexander Weiss. *A Survey of Challenges for Runtime Verification from Advanced Application Domains (Beyond Software)*. Formal Methods in System Design, Vol. 54, Num. 3, pages 279–335, November 2019.
5. Aleksandar Nanevski, Anindya Banerjee, Germán Andrés Delbianco, Ignacio Fábregas. *Specifying Concurrent Programs in Separation Logic: Morphisms and Simulations*. PACMPL, Vol. 3, Num. OOPSLA, pages 1–30, ACM, October 2019.
6. Joaquín Arias, Manuel Carro. *Evaluation of the Implementation of an Abstract Interpretation Algorithm Using Tabled CLP*. Theory



and Practice of Logic Programming, Vol. 19, Num. 5-6, pages 1107–1123, September 2019. Special Issue on ICLP'19.

7. Jesús J. Doménech, John P. Gallagher, Samir Genaim. *Control-Flow Refinement by Partial Evaluation, and its Application to Termination and Cost Analysis*. TPLP, Vol. 19, Num. 5-6, pages 990–1005, Cambridge University Press, September 2019.
8. Gilles Barthe, Gustavo Betarte, Juan Diego Campo, Carlos Luna. *System-Level Non-interference of Constant-Time Cryptography. Part I: Model*. Journal of Automated Reasoning, Vol. 63, Num. 1, pages 1–51, June 2019.
9. Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, Elena Pagnin. *Multi-key Homomorphic Authenticators*. IET Information Security, Vol. 13, Num. 6, pages 618–638, Institution of Engineering and Technology, April 2019.
10. Gilles Barthe, Edvard Fagerholm, Dario Fiore, John C. Mitchell, Andre Scedrov, Benedikt Schmidt. *Automated Analysis of Cryptographic Assumptions in Generic Group Models*. Journal of Cryptology, Vol. 32, Num. 2, pages 324–360, April 2019.
11. Gilles Barthe, Christos Dimitrakakis, Marco Gaboardi, Andreas Haeberlen, Aaron Roth, Aleksandra B. Slavkovic. *Program for TPD 2016*. Journal of Privacy and Confidentiality, Vol. 9, Num. 1, March 2019.
12. Pablo Cañones, Boris Köpf, Jan Reineke. *On the Incomparability of Cache Algorithms in Terms of Timing Leakage*. Logical Methods in Computer Science, Vol. 15, Num. 1, March 2019.
13. Patrick Cousot, Roberto Giacobazzi, Francesco Ranzato. *AI: Abstract Interpretation*. PACMPL, Vol. 3, Num. POPL, pages 1–31, ACM, January 2019.
14. Tetsuya Sato, Alejandro Aguirre, Gilles Barthe, Marco Gaboardi, Deepak Garg, Justin Hsu. *Formal Verification of Higher-Order Probabilistic Programs: Reasoning About Approximation, Convergence, Bayesian Inference, and Optimization*. Proc. ACM Program. Lang., Vol. 3, Num. POPL, pages 1–30, ACM, January 2019.
15. Richard Rivera, Platon Kotzias, Avinash Sudhodanan, Juan Caballero. *Costly Free-ware: A Systematic Analysis of Abuse in Download Portals*. IET Information Security, Vol. 13, Num. 1, pages 27–35, IET, January 2019.
16. James Parker, Niki Vazou, Michael Hicks. *LWeb: Information Flow Security for Multi-tier Web Applications*. PACMPL, Vol. 3, Num. POPL, pages 1–30, 2019.
17. Luca Aceto, Ignacio Fábregas, Álvaro García-Pérez, Anna Ingólfssdóttir, Yolanda Ortega-Mallén. *Rule Formats for Nominal Process Calculi*. Logical Methods in Computer Science, Vol. 15, Num. 4, 2019.
18. Luca Aceto, Ignacio Fábregas, Carlos Gregorio-Rodríguez, Anna Ingólfssdóttir. *Logical Characterisations, Rule Formats and Compositionality for Input-Output Conformance Simulation*. J. Log. Algebr. Meth. Program., Vol. 106, pages 78–106, 2019.
19. Luca Aceto, Dario Della Monica, Ignacio Fábregas, Anna Ingólfssdóttir. *When Are Prime Formulae Characteristic?*. Theor. Comput. Sci., Vol. 777, pages 3–31, 2019.
20. Antonio Faonio, Jesper Buus Nielsen, Mark Simkin, Daniele Venturi. *Continuously Non-malleable Codes with Split-State Refresh*. Theoretical Computer Science, Vol. 759, pages 98–132, 2019.



21. Alejandro Aguirre, Gilles Barthe, Marco Gaboardi, Deepak Garg, Pierre-Yves Strub. *A Relational Logic for Higher-Order Programs*. Journal of Functional Programming, Vol. 29, Cambridge University Press, 2019.
22. Julio Mariño, Raúl N. N. Alborodo, Lars-Åke Fredlund, Ángel Herranz-Nieva. *Synthesis of Verifiable Concurrent Java Components from Formal Models*. Software and Systems Modeling, Vol. 18, Num. 1, pages 71–105, 2019.
23. Joaquín Arias, Manuel Carro. *Description, Implementation, and Evaluation of a Generic Design for Tabled CLP*. Theory and Practice of Logic Programming, Vol. 19, Num. 3, pages 412–448, Cambridge U. Press, 2019.
24. Zorana Vanković, Umer Liqat, Pedro Lopez-Garcia. *A General Methodology for Energy-Efficient Scheduling in Multicore Environments Based on Evolutionary Algorithms*. Journal of Multiple-Valued Logic and Soft Computing (JMVLS), SOCO'15 Special Issue, Vol. 32, Num. 3-4, pages 313–341, Old City Publishing, 2019.
25. Álvaro García-Pérez, Pablo Nogueira. *The Full-Reducing Krivine Abstract Machine KN Simulates Pure Normal-Order Reduction in Lockstep: A Proof via Corresponding Calculus*. Journal of Functional Programming, Vol. 29, Num. E7, pages 1–38, Cambridge University Press, 2019.
26. Zolt István. *The Glass Half Full: Using Programmable Hardware Accelerators in Analytics*. IEEE Data Eng. Bull., Vol. 42, Num. 1, pages 49–60, 2019.
27. Gustavo Alonso, Zolt István, Kaan Kara, Muhsen Owaida, David Sidler. *doppioDB 1.0: Machine Learning inside a Relational Engine*. IEEE Data Engineering, Vol. 42, Num. 2, pages 19–31, 2019.

Conferences

1. Borja Balle, Gilles Barthe, Marco Gaboardi, Joseph Geumlek. *Privacy Amplification by Mixing and Diffusion Mechanisms*. Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems (NeurIPS 2019), pages 13277–13287, December 2019.
2. Gianluca Brian, Antonio Faonio, Daniele Venturi. *Continuously Non-malleable Secret Sharing for General Access Structures*. Theory of Cryptography - 17th International Conference, TCC 2019, Proceedings, Part II, Lecture Notes in Computer Science, Vol. 11892, pages 211–232, Springer, December 2019.
3. José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Matthew Campagna, Ernie Cohen, Benjamin Grégoire, Vitor Pereira, Bernardo Portela, Pierre-Yves Strub, Serdar Tasiran. *A Machine-Checked Proof of Security for AWS Key Management Service*. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, pages 63–78, ACM, November 2019.
4. José Bacelar Almeida, Cecile Baritel-Ruet, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Alley Stoughton, Pierre-Yves Strub. *Machine-Checked Proofs for Cryptographic Standards: Indifferentiability of Sponge and Secure High-Assurance Implementations of SHA-3*. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, pages 1607–1622, ACM, November 2019.
5. Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Mélissa Rossi, Mehdi Tibouchi. *GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time*





- Implementation of Cryptographic Signatures, Revisited*. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, pages 2147–2164, ACM, November 2019.
6. Piotr Mardziel, Niki Vazou. *PLAS 2019: ACM SIGSAC Workshop on Programming Languages and Analysis for Security*. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, November 2019.
 7. Antonio Faonio, Dario Fiore, Javier Heranz, Carla Ràfols. *Structure-Preserving and Re-randomizable RCCA-Secure Public Key Encryption and its Applications*. ASIA-CRYPT 2019: 25th Annual International Conference on the Theory and Applications of Cryptology and Information Security, LNCS, Springer, November 2019.
 8. Matteo Campanelli, Dario Fiore, Anaïs Querol. *LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs*. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, pages 2075–2092, ACM, November 2019.
 9. Ignacio Cascudo, Ivan Damgård, Bernardo David, Nico Döttling, Rafael Dowsley, Irene Giacomelli. *Efficient UC Commitment Extension with Homomorphism for Free (and Applications)*. Advances in Cryptology - ASIA-CRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, November 2019.
 10. Marco Campion, Mila Dalla Preda, Roberto Giacobazzi. *Abstract Interpretation of Indexed Grammars*. Static Analysis - 26th International Symposium, SAS 2019, Lecture Notes in Computer Science, Vol. 11822, pages 121–139, Springer, October 2019.
 11. Gilles Barthe, Renate Eilers, Pamina Georgiou, Bernhard Gleiss, Laura Kovács, Matteo Maffei. *Verifying Relational Properties Using Trace Logic*. Formal Methods in Computer Aided Design, FMCAD 2019, pages 170–178, IEEE, October 2019.
 12. Artem Khyzha, Hagit Attiya, Alexey Gotsman. *Privatization-Safe Transactional Memories*. DISC'19: International Symposium on Distributed Computing, LIPICS, Vol. 146, pages 1–17, Dagstuhl, October 2019.
 13. Luis Miguel Danielsson, César Sánchez. *Decentralized Stream Runtime Verification*. Proc. of the 19th Int'l Conf. on Runtime Verification (RV'19), Lecture Notes in Computer Science, Vol. 11757, pages 185–201, Springer, October 2019.
 14. Martin Leucker, César Sánchez, Torben Scheffel, Malte Schmitz, Daniel Thoma. *Runtime Verification for Timed Event Streams with Partial Information*. Proc. of the 19th Int'l Conf. on Runtime Verification (RV'19), Lecture Notes in Computer Science, Vol. 11757, pages 273–291, Springer, October 2019.
 15. Gilles Barthe, Sonia Belaïd, Gaëtan Casiers, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert. *maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults*. Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Proceedings, Part I, Lecture Notes in Computer Science, Vol. 11735, pages 300–318, Springer, September 2019.
 16. Manuel Bravo, Alexey Gotsman. *Reconfigurable Atomic Transaction Commit*. PODC'19: Symposium on Principles of Distributed Computing, pages 399–408, ACM Press, August 2019.



17. Iskander Sánchez-Rola, Matteo Dell'Amico, *Platon Kotzias*, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, Igor Santos. *Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control*. Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, AsiaCCS 2019, pages 340–351, ACM, July 2019.
18. Gilles Barthe, Benjamin Grégoire, Charlie Jacomme, Steve Kremer, *Pierre-Yves Strub*. *Symbolic Methods in Computational Cryptography Proofs*. 32nd IEEE Computer Security Foundations Symposium, CSF 2019, pages 136–151, IEEE, June 2019.
19. Tetsuya Sato, *Gilles Barthe*, Marco Gaboardi, Justin Hsu, Shin-ya Katsumata. *Approximate Span Liftings: Compositional Semantics for Relaxations of Differential Privacy*. 34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, pages 1–14, IEEE, June 2019.
20. Sunjay Cauligi, Gary Soeller, Brian Johannesmeyer, Fraser Brown, Riad S. Wahby, John Renner, Benjamin Grégoire, *Gilles Barthe*, Ranjit Jhala, Deian Stefan. *FaCT: A DSL for Timing-Sensitive Computation*. Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2019, pages 174–189, ACM, June 2019.
21. Ezgi Çiçek, Weihao Qu, *Gilles Barthe*, Marco Gaboardi, Deepak Garg. *Bidirectional Type Checking for Relational Properties*. Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2019, pages 533–547, ACM, June 2019.
22. Alexey Gotsman, Anatole Lefort, Gregory Chockler. *White-Box Atomic Multicast*. DSN'19: International Conference on Dependable Systems and Networks, pages 176–187, IEEE Press, June 2019.
23. Pepe Vila, Boris Köpf, Jose Morales. *Theory and Practice of Finding Eviction Sets*. Proc. 40th IEEE Symposium on Security and Privacy (S&P '19), pages 39–54, IEEE, May 2019.
24. John P. Gallagher. *Polyvariant Program Specialisation with Property-Based Abstraction*. Proceedings Seventh International Workshop on Verification and Program Transformation (VPT), EPTCS, Vol. 299, pages 34–48, April 2019.
25. *Platon Kotzias*, Leyla Bilge, Pierre-Antoine Vervier, Juan Caballero. *Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises*. Network and Distributed Systems Security Symposium, February 2019.
26. Joaquín Arias, Manuel Carro. *Incremental Evaluation of Lattice-Based Aggregates in Logic Programming Using Modular TCLP*. 21st Int'l. Symposium on Practical Aspects of Declarative Languages, LNCS, Vol. 11372, pages 98–114, Springer, January 2019.
27. I. Garcia-Contreras, J.F. Morales, M. V. Hermenegildo. *Multivariant Assertion-Based Guidance in Abstract Interpretation*. Proceedings of the 28th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'18), LNCS, Num. 11408, pages 184–201, Springer-Verlag, January 2019.
28. Marco Guarnieri, Musard Balliu, Daniel Schoepe, David Basin, Andrei Sabelfeld. *Information-Flow Control for Database-Backed Applications*. Proceedings of the 4th IEEE European Symposium on Security and Privacy, EuroS&P 2019, IEEE, 2019.





29. Milod Kazerounian, Sankha Narayan Guria, Niki Vazou, Jeffrey S. Foster, David Van Horn. *Type-Level Computations for Ruby Libraries*. Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI, pages 966–979, ACM, 2019.
30. Pedro Joaquim, Manuel Bravo, Luís E. T. Rodrigues, Miguel Matos. *Hourglass: Leveraging Transient Resources for Time-Constrained Graph Processing in the Cloud*. Proceedings of the Fourteenth EuroSys Conference, pages 1–16, ACM, 2019.
31. Antonio Faonio, Daniele Venturi. *Non-malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate*. Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Lecture Notes in Computer Science, Vol. 11693, pages 448–479, Springer, 2019.
32. Sandro Coretti, Antonio Faonio, Daniele Venturi. *Rate-Optimizing Compilers for Continuously Non-malleable Codes*. Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Lecture Notes in Computer Science, Vol. 11464, pages 3–23, Springer, 2019.
33. Antonio Faonio. *Efficient Fully-Leakage Resilient One-More Signature Schemes*. Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference, Lecture Notes in Computer Science, Vol. 11405, pages 350–371, Springer, 2019.
34. Pierre Ganty, Francesco Ranzato, Pedro Valero. *Language Inclusion Algorithms as Complete Abstract Interpretations*. Static Analysis - 26th International Symposium, SAS 2019, Lecture Notes in Computer Science, Vol. 11822, pages 140–161, Springer, 2019.
35. Pierre Ganty, Elena Gutiérrez, Pedro Valero. *A Congruence-Based Perspective on Automata Minimization Algorithms*. 44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, LIPIcs, Vol. 138, pages 1–14, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.
36. Pierre Ganty, Pedro Valero. *Regular Expression Search on Compressed Text*. 2019 Data Compression Conference (DCC), pages 528–537, IEEE, 2019.
37. Norine Coenen, Bernd Finkbeiner, César Sánchez, Leander Tentrup. *Verifying Hyperliveness*. Proc. of the 31st Int'l Conf. on Computer Aided Verification (CAV'19), Lecture Notes in Computer Science, Vol. 11561, pages 121–139, Springer, 2019.
38. Sandro Stucki, César Sánchez, Gerardo Schneider, Borzoo Bonakdarpour. *Gray-Box Monitoring of Hyperproperties*. Formal Methods - The Next 30 Years - Third World Congress, FM 2019, Lecture Notes in Computer Science, Vol. 11800, pages 406–424, Springer, 2019.
39. Álvaro García-Pérez, Maria A. Schett. *Deconstructing Stellar Consensus*. 23rd International Conference on Principles of Distributed Systems (OPODIS 2019), LIPIcs, Vol. 153, pages 1–16, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.
40. Haggai Eran, Lior Zeno, Zsolt István, Mark Silberstein. *Design Patterns for Code Reuse in HLS Packet Processing Pipelines*. 2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), pages 208–217, IEEE, 2019.



Workshops

1. I. Casso, J. F. Morales, P. Lopez-Garcia, R. Giacobazzi, M. V. Hermenegildo. *Computing Abstract Distances in Logic Programs*. Pre-proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), November 2019.
2. I. Casso, J. F. Morales, P. Lopez-Garcia, M. V. Hermenegildo. *An Integrated Approach to Assertion-Based Random Testing in Prolog*. Pre-proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), November 2019.
3. M. Klemen, P. Lopez-Garcia, J. Gallagher, J.F. Morales, M. V. Hermenegildo. *A General Framework for Static Cost Analysis of Parallel Logic Programs*. Pre-proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), November 2019.
4. I. Garcia-Contreras, J.F. Morales, M. V. Hermenegildo. *Experiments in Context-Sensitive Incremental and Modular Static Analysis in CiaoPP*. 10th Workshop on Tools for Automatic Program Analysis (TAPAS'19), October 2019. (Extended Abstract).
5. I. Garcia-Contreras, J.F. Morales, M. V. Hermenegildo. *Incremental Analysis of Logic Programs with Assertions and Open Predicates*. Pre-proceedings of the 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'19), October 2019.
6. J. Arias, Z. Chen, M. Carro, G. Gupta. *Modeling and Reasoning in Event Calculus Using Goal-Directed Constraint Answer Set Programming*. Pre-Proc. of the 29th Int'l. Symposium on Logic-based Program Synthesis and Transformation, September 2019.
7. M. Klemen, P. Lopez-Garcia, J. Gallagher, J.F. Morales, M. V. Hermenegildo. *Towards a General Framework for Static Cost Analysis of Parallel Logic Programs*. Technical Communications of the 35th International Conference on Logic Programming (ICLP 2019), Electronic Proceedings in Theoretical Computer Science (EPTCS), pages 238–240, Open Publishing Association (OPA), September 2019. (Extended Abstract).
8. I. Casso, J. F. Morales, P. Lopez-Garcia, M. V. Hermenegildo. *Towards Computing Abstract Distances in Logic Programs*. Technical Communications of the 35th International Conference on Logic Programming (ICLP 2019), Electronic Proceedings in Theoretical Computer Science (EPTCS), pages 65–66, Open Publishing Association (OPA), September 2019. (Extended Abstract).
9. Joaquín Arias, Manuel Carro, Zhuo Chen, Gopal Gupta. *Constraint Answer Set Programming without Grounding and its Applications*. 3rd Int'l. Workshop on the Resurgence of Datalog in Academia and Industry (Datalog 2.0), Vol. 2368, pages 22–26, CEUR-WS, June 2019.
10. Arianna Blasi, Mauro Pezzè, Alessandra Gorla, Michael D. Ernst. *Research on NLP for RE at Università della Svizzera Italiana (USI): A Report*. Joint Proceedings of REFSQ-2019 Workshops, Doctoral Symposium, Live Studies Track, and Poster Track co-located with the 25th International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2019), CEUR Workshop Proceedings, Vol. 2376, CEUR-WS.org, 2019.
11. Daniel Domínguez-Álvarez, Alessandra Gorla. *Release Practices for iOS and Android Apps*. Proceedings of the 3rd ACM SIGSOFT International Workshop on App Market Analytics, WAMA-ESEC/SIGSOFT FSE 2019, pages 15–18, ACM, 2019.





12. Lucas Kuhring, Eva Garcia, Zsolt István. *Specialize in Moderation: Building Application-Aware Storage Services Using FPGAs in the Datacenter*. 11th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 19), 2019.
13. Claudio Ferretti, Alberto Leporati, Luca Mariot, Luca Nizzardo. *Transferable Anonymous Payments via TumbleBit in Permissioned Blockchains*. Proceedings of the Second Distributed Ledger Technology Workshop, DLT-ITASEC 2019, CEUR Workshop Proceedings, Vol. 2334, pages 56–67, CEUR-WS.org, 2019.
3. Pablo Cañones Martín. *On the Security of Cache Algorithms*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2019. Advisor: Boris Koepf (IMDEA Software Institute).
4. Paolo Calciati. *Understanding the Evolution of Android Applications*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). November 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).
5. Platon Kotzias. *A Systematic Empirical Analysis of Unwanted Software Abuse, Prevalence, Distribution, and Economics*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). May 2019. Advisor: Juan Caballero (IMDEA Software Institute).
6. Raúl Alborodo. *A Model Driven Methodology for the Construction of Reliable Concurrent Software*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). December 2019. Advisor: Julio Mariño Carballo (UPM).
7. Ankita Israel Sadu. *Automatic Detection of Outdated Comments in Open-Source Java Projects*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).
8. Daniel Domínguez Álvarez. *Checking Android Applications Behaviour against Google Play Descriptions at Scale*. Master Thesis. Universidad Politécnica de Madrid (UPM). January 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).
9. Daniel Toniuc. *An Automated Analysis of the “What’s New” Descriptions of Android Apps*. Master Thesis. Universidad Politécnica de Madrid (UPM). June 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).

Edited Volumes

1. Pierre Ganty, Mohamed Kaâniche (Eds.). *Verification and Evaluation of Computer and Communication Systems - 13th International Conference, VECoS 2019, Proceedings*. Lecture Notes in Computer Science, Vol. 11847, Springer, October 2019.
2. Alessandra Gorla, José Miguel Rojas (Eds.). *Proceedings of the 12th International Workshop on Search-Based Software Testing, SBST-ICSE 2019*. IEEE / ACM, 2019.

Doctoral, Master and Bachelor Theses

1. Anca Nitulescu. *A Tale of SNARKs: Quantum Resilience, Knowledge Extractability and Data Privacy*. Ph.D. Thesis. École Normale Supérieure. April 2019. Advisors: Dario Fiore (IMDEA Software Institute), David Pointcheval and Michel Abdalla.
2. Irfan Ul Haq. *Lineage Inference of Packed Malware Using Binary Code Similarity*. Ph.D. Thesis. Universidad Politécnica de Madrid



10. Harry Alberto Carpio Salvatierra. *A Proposal of Automatic Quality Evaluator for GIT Commit Messages*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).
11. Jorge Blázquez Díaz. *Threshold Decryption Protocols for (Replayable) Chosen Cipher-text Secure Public Key Encryption*. Master Thesis. Universidad Complutense de Madrid (UCM). September 2019. Advisors: Dario Fiore and Antonio Faonio (IMDEA Software Institute).
12. Soheil Khodayari. *A Framework for Testing Web Applications for Cross-Origin State Inference (COSI) Attacks*. Master Thesis. Universidad Politécnica de Madrid (UPM). June 2019. Advisors: Avinash Sudhodanan and Juan Caballero (IMDEA Software Institute).
13. Stefano Ottolenghi. *Homomorphic Signatures over Lattices*. Master Thesis. Università degli Studi di Genova. September 2019. Advisor: Dario Fiore (IMDEA Software Institute).
14. Andrés Sánchez Marín. *Detecting Speculative Information-Flows in Large Code Bases*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). June 2019. Advisors: Marco Guarnieri and José Francisco Morales (IMDEA Software Institute).
15. Jose Carlos Garde González. *Análisis de las Características de las Herramientas de Testing Automático de Aplicaciones Android de la Plataforma Androtest on Docker*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). January 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).
16. Guillermo Paredes López. *Herramienta de Actualización Automática de Tests para Android*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). January 2019. Advisor: Alessandra Gorla (IMDEA Software Institute).





Invited Talks

Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Advances in computer-aided cryptography. LatinCrypt 2019, Santiago de Chile, October 2019.
2. *Gilles Barthe*. Formal verification of side-channel countermeasures. CARDIS'19, Prague, November 2019.
3. *Juan Caballero*. Malware Similarity: Reuse, Lineage, Attribution. Invited keynote at TrendMicro Experts Summit (TES). Cebu, Philippines. April 2019.
4. *Manuel Carro*. AI now: it really fits! EIT Digital Spain, Innovation Day 2019. Madrid, Spain, December 2019.
5. *Dario Fiore*. LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs. 2nd ZKProof Workshop, Berkeley, California, US, April 2019.
6. *John Gallagher*. Horn clauses and tree automata for imperative program verifica-

tion. 29th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 19), Porto, Portugal, October 2019.

7. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. Workshop on Verification of Distributed Systems (VDS). Marrakesh, Morocco, June 2019.
8. *Alexey Gotsman*. Reasoning about consistency choices in modern distributed systems. Summer School on Verification Technology, Systems & Applications. University of Luxembourg, July 2019.
9. *M.V. Hermenegildo*. Assertion-based Guidance of Top-down Horn Clause-based Analysis in CiaoPP. Invited talk at Workshop on Declarative Program Analysis (DPA 2019, associated to PLDI). Phoenix, Arizona, USA, June 2019.

Invited Seminars and Lectures by IMDEA Scientists

1. *Alejandro Aguirre*. Almost Sure Productivity. National Institute of Informatics. Tokyo, Japan, April 2020.
2. *Alejandro Aguirre*. A higher-order logic for adversarial computations. National Institute of Informatics. Tokyo, Japan, April 2020.
3. *Joaquín Arias*. Contribution of my Thesis and Spatial Reasoning in Building Information Modeling using CLP. Aalto University (BIM Lab). Helsinki, Finland, August 2019.
4. *Matteo Campanelli*. How to Verify Computation in the Blink of an Eye. Universidad Complutense de Madrid. Madrid, Spain. July 2019.
5. *Matteo Campanelli*. LegoSNARK: Composing ZKPs Simply and Efficiently. ZKProof Com-



- community Event, Amsterdam, The Netherlands. October 2019.
6. *Manuel Carro*. Investigación e Innovación en Madrid. El papel de los Institutos y Centros de I+D. Misión y modelos de organización. Universidad Politécnica de Madrid: Innovación e I+D en Tecnologías Emergentes para la Transformación Digital. Madrid, Spain. January 2019.
7. *Manuel Carro*. Programas horizontales de Horizon 2020: el *European Institute of Innovation and Technology*. Universidad Politécnica de Madrid, Postgraduate degree on Project Management. Madrid, Spain. March 2019.
8. *Manuel Carro*. Blockchain: Tecnología y aplicaciones. Escuela de Organización Industrial, Executive MBA. Madrid, Spain. November 2019.
9. *Ignacio Cascudo*. Applications of error correcting codes in secure multiparty computation. International Congress of Industrial and Applied Mathematics, Valencia, Spain, 17 July 2019.
10. *Ignacio Cascudo*. Squares of cyclic codes. 13th Nordic Combinatorial Conference, Copenhagen, Denmark, 6 August 2019.
11. *Alvaro García*. Federated Byzantine Quorum Systems. Seminar of the Information Security Group at University College London (UCL), UK, January 2019.
12. *Alvaro García*. Federated Byzantine Quorum Systems. BART Blockchain Seminar, Telecom ParisTech, Paris, France, February 2019.
13. *Dario Fiore*. Homomorphic Authentication for Computing Securely on Untrusted Machines. Paris Crypto Day, Paris, France, March 2019.
14. *Dario Fiore*. Homomorphic Authentication for Computing Securely on Untrusted Machines. University of Verona, Italy, May 2019.
15. *Dario Fiore*. LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs. BBVA, Madrid, Spain, May 2019.
16. *Dario Fiore*. LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs. ICIAM 2019, Valencia, Spain, July 2019.
17. *John Gallagher*. Horn clauses for imperative program verification. Dept. of Computer Science, Katholieke Universiteit Leuven, Leuven, Belgium, September, 2019.
18. *Pierre Ganty*. Deciding language inclusion problems using quasiorders. Verification Seminar of IRIF, Paris, France, October 2019.
19. *Pierre Ganty*. Deciding language inclusion problems using quasiorders. ConVeY talk TU Munich, Germany, November 2019.
20. *Alessandra Gorla*. Inferring procedure specifications from Javadoc comments for automated testing. Universidad Complutense de Madrid, Spain, April 2019.
21. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. IST Lisbon, Portugal, January 2019.
22. *Alexey Gotsman*. State-Machine Replication for Planetary-Scale Systems. University of Washington, USA, February 2019.
23. *Alexey Gotsman*. State-Machine Replication for Planetary-Scale Systems. Microsoft Research Redmond, USA, February 2019.
24. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. VMware Research, USA, March 2019.
25. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. University of Lugano, Switzerland, May 2019.





26. *Marco Guarnieri*. Principled detection of speculative information flows. Ruhr-Universität Bochum, March 2019.
27. *Marco Guarnieri*. Spectector: Principled detection of speculative information flows. Intel Side Channel Academic Program Workshop, June 2019.
28. *Marco Guarnieri*. Spectector: Principled detection of speculative information flows. Microsoft Research Cambridge, November 2019.
29. *Elena Gutiérrez*. ¿Cómo garantizar que un programa hace lo que esperas? I+D+M. Mujeres en Montegancedo. Madrid, Spain. February 2019.
30. *Zsolt István*. Introduction to FPGA-accelerated computation. UTCN Cluj, Romania, April 2019.
31. *Zsolt István*. Past and future challenges of analytic database acceleration with FPGAs. UCM Madrid, Spain, May 2019.
32. *Zsolt István*. Past and future challenges of analytic database acceleration with FPGAs. UPM Madrid, Spain, June 2019.
33. *Zsolt István*. Specialize in Moderation: Building Application-aware Storage Services using FPGAs in the Datacenter. Imperial College London, UK. July 2019.
34. *Zsolt István*. StreamChain: Towards Sub-Millisecond Processing in Blockchains. ETH Zurich, Switzerland, November 2019.
35. *Zsolt István*. Past and future challenges of analytic database acceleration with FPGAs. SAP Walldorf, Germany, November 2019.
36. *Zsolt István*. Introduction to hardware-accelerated consensus. UTCN Cluj, Romania, December 2019.
37. *Zsolt István*. Introduction to FPGA-accelerated computation. UTCN Cluj, Romania, December 2019.
38. *Dimitris Kolonelos*. Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular. Cryptoeconomics Security Conference 2019 (CESC), San Francisco, USA, October 2019.
39. *Anaïs Querol*. STARKs on an Eggshell. ZKProof Community Event. Amsterdam, The Netherlands, October 2019.
40. *César Sánchez*. Stream Runtime Verification Revisited. Workshop on Continuous Observation of Embedded Multicore Systems (COEMS), Valencia, Spain. January 2019.
41. *César Sánchez*. Stream Runtime Verification. STINT Workshop on Runtime Verification and Autonomous Systems, University of Gothenburg, Sweden. August 2019.
42. *César Sánchez*. An Introduction to (Stream) Runtime Verification. SRV Tutorial (collocated with Formal Methods 2019), Porto, Portugal. October 2019.
43. *Niki Vazou*. Liquidate your Assets. IFIP WG2.8 Meeting 2019. Bordeaux, France. May 2019.
44. *Niki Vazou*. Theorem Proving in Haskell. 12th Panhellenic Logic Symposium. Anogeia, Crete, Greece. June 2019.
45. *Niki Vazou*. Types and Verification. Programming Language Mentoring Workshop @ ICFP 2019. Berlin, Germany. August 2019.
46. *Niki Vazou*. Liquidate your Assets. Summer BOB 2019. Berlin, Germany. August 2019.
47. *Pepe Vila*. Cache and Syphilis. RootedCON 2019. Madrid, Spain. March 2019.



Invited Speaker Series

During 2019, 35 external speakers were invited to give talks at IMDEA Software. All of our seminars and talks are open to the campus and the academic community at large. The following list shows the speakers and the titles of their talks.

1. *Julian Thomé*. Junior researcher, ShiftLeft: Automated Security Code Analysis Made Easy.
2. *Miguel Á. Carreira-Perpiñán*. Professor, University of California at Merced, USA: A new way to train decision trees: tree alternating optimization (TAO).
3. *Michael D. Adams*. Software Engineer, The University of Utah, USA: Advances in Parsing.
4. *Eduardo Bezerra*. Software Engineer, Amazon Madrid: Strong Consistency at Scale.
5. *Martin A.T. Handley*. PhD Student, University of Nottingham, United Kingdom: Liquidate your assets: reasoning about resource usage in Liquid Haskell.
6. *Rahul Chatterjee*. PhD Student, Cornell University, New York, USA: Empiricism-Informed Secure System Design: From Improving Passwords to Helping Domestic Violence Victims.
7. *Paolo Giarrusso*. Post-doctoral Researcher, EPFL, Switzerland: Towards Semantic Type Soundness for Dependent Object Types and Scala with Logical Relations in Iris.
8. *Andreas Pavlogiannis*. Post-doctoral Researcher, EPFL, Switzerland: Algorithmic Advances in Automated Program Analysis.
9. *Joseph Izraelevitz*. Post-doctoral Researcher, UC San Diego: Practical and Formal Infrastructure for Nonvolatile Memory.
10. *Ingo Mueller*. Post-doctoral Researcher, ETH Zurich, Switzerland: The State of the Art of Data Analytics Systems and What is Wrong about it.
11. *Marko Vukolić*, Researcher. IBM Research - Zurich: Hyperledger Fabric: a Distributed Operating System for Permissioned Blockchains.
12. *Kenji Maillard*. PhD Student, INRIA Paris, France: Designing Dijkstra Monads.
13. *Maria Schett*. PhD Student, University College London, United Kingdom: Blockchain Superoptimizer.
14. *Joao Marques Silva*. Research Professor, Universidade de Lisboa: Logic-Enabled Explanations for Machine Learning Models.
15. *Marco Guarnieri*. Post-doctoral Researcher, IMDEA Software Institute: Principled detection of speculative information flows.
16. *Klaus von Gleissenthall*. Post-doctoral Researcher, UC San Diego: Pretend Synchrony: Synchronous Verification of Asynchronous Distributed Programs.
17. *Ignacio Cascudo*. Associate Professor, Aalborg University, Denmark: Some developments in secure multiparty computation for binary circuits.
18. *František Farka*. PhD Student, Heriot-Watt University, United Kingdom: Proof-Relevant Resolution: The Foundations of Constructive Automation.
19. *Mooly Sagiv*. Research Professor, Tel Aviv University, Israel: Deductive verification of distributed protocols in first-order logic.
20. *Antonio Nappa*. Researcher, Brave Software: Trusted Hardware: The Good, The Bad, The Ugly.





21. *Yotam Feldman*. PhD Student, Tel Aviv University, Israel: Order out of Chaos: Proving Linearizability Using Local Views.
22. *Yotam Feldman*. PhD Student, Tel Aviv University, Israel: Inferring Inductive Invariants from Phase Structures.
23. *Gregory Chockler*. Research Professor, Royal Holloway, University of London (RHUL): Atomic Transaction Commit for Modern Data Stores.
24. *Christian Roldán*. PhD Student, University of Buenos Aires, Argentina: About semantics of replicated data stores.
25. *Alejandro Ranchal-Pedrosa*. PhD Student, University of Sydney, Australia: Platypus: Offchain Protocols without Synchrony.
26. *Yu-yang Lin*. PhD Student, Queen Mary, London University: A Bounded Model Checking Technique for Higher-Order Programs.
27. *Bernardo David*. Associate Professor, IT University of Copenhagen, Denmark: Efficient Privacy Preserving Computation meets Blockchains.
28. *Veronica Dahl*. Research Professor, Simon Fraser University, Canada: AI for Social Responsibility: Embedding principled guidelines into AI systems.
29. *Ignacio Luengo*. Professor, Universidad Complutense de Madrid, Spain: Post-quantum Cryptography with polynomials.
30. *Giovanni Denaro*. Associate Professor, University of Milano-Bicocca, Italy: Automatic Test Generation for Programs with Complex Structured Inputs.
31. *Jan Tretmans*. Associate Professor, Radboud University, The Netherlands: Goodbye ioco, hello uioco.
32. *Roberto Bagnara*. Professor, University of Parma, Italy: MISRA C and its key role for the compliance to industrial safety standards.
33. *Antonio Nappa*. Researcher, Corelight Inc, USA: ZKSENSE: a Privacy-Preserving Mechanism for Bot Detection in Mobile Devices.
34. *Nazareno Aguirre*. Associate Professor, Universidad Nacional de Río IV, Argentina: Tight Bounds and Applications in Generalized Symbolic Execution and Test Input Generation.

Software Seminar Series

1. The Institute also holds an internal seminar series to foster communication and collaboration. A total of **24** seminars were given in 2019.





Scientific Service and Other Activities

Conference and Program Committee Chairmanship

Pierre Ganty:

1. PC Co-Chair, 13th International Conference on Verification and Evaluation of Computer and Communication Systems (VECoS 2019).

Alessandra Gorla:

2. PC Co-Chair, 11th International Workshop on Search-Based Software Testing (SBST 2019).
3. Co-Chair, 2019 ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2019), tool demo track.
4. Co-Chair, 2019 IEEE International Conference on Software Testing, Verification and Validation (ICST 2019), tool demo track.

Zsolt István:

5. Co-organizer and PC Chair, Workshop on Systems for Multi-core and Heterogeneous Architectures, co-located with EuroSys 2019.
6. Co-organizer and PC Chair of Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, co-located with Middleware 2019.

Manuel Hermenegildo:

7. PC Co-Chair (and co-organizer) of the 2019 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation (PEPM).

César Sánchez:

8. PC Co-Chair, PhD Symposium of the 15th International Conference on Integrated Formal Methods (PhD-iFM 2019).

Niki Vazou:

9. Co-Chair, ACM SIGSAC 14th Workshop on Programming Languages and Analysis for Security (PLAS 2019).
10. Chair of Student Research Competition, 46th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2019).
11. Chair, of Haskell Implementor's Workshop 2019.

Editorial Boards and Conference Steering Committees

Gilles Barthe:

1. Editorial Board of the Journal of Automated Reasoning.
2. Editorial Board of the Journal of Computer Security.
3. Editorial board of Transactions on Dependable and Secure Computing.

Juan Caballero:

4. Editorial Board of the ACM Transactions in Privacy and Security (ACM TOPS).
5. Steering committee of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).
6. Steering Committee of the International Symposium on Engineering Secure Software and Systems (ESSoS).

Manuel Carro:

7. Area Editor, Theory and Practice of Logic Programming.



**Dario Fiore:**

8. Editorial Board of IET Information Security Journal.
9. Editor Board of the International Journal of Applied Cryptography.

John Gallagher:

10. Steering Committee. International Symposium on Functional and Logic Programming (FLOPS).

Alessandra Gorla:

11. Steering Committee. International Workshop on Search-Based Software Testing (SBST).

Manuel Hermenegildo:

12. Steering Committee of the Conference on Compiler Construction (CC).
13. Steering Committee of the International Symposium on Functional and Logic Programming (FLOPS).
14. Steering Committee of the International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR).
15. Editorial Advisor of "Theory and Practice of Logic Programming" (Cambridge U. Press).
16. Associate Editor of the "Journal of New Generation Computing" (Springer-Verlag).
17. Area Editor of the "Journal of Applied Logic" (Elsevier North-Holland).
18. Area editor, Algorithms in Programming Languages and Software Engineering, of the "Journal of the IGPL" (Oxford U press).

Niki Vazou:

19. Steering Committee of Haskell Symposium.
20. Steering Committee of ACM SIGSAC Workshop on Programming Languages and Analysis for Security (PLAS).
21. Steering Committee of Workshop on Type-driven Development (TyDe).

Participation in Program Committees**Gilles Barthe:**

1. 26th ACM Conference on Computer and Communications Security (CCS 2019).
2. 31st International Conference on Computer-Aided Verification (CAV 2019).
3. 3rd World Congress on Formal Methods (FM 2019).

Manuel Bravo:

4. 6th Workshop in Principles and Practice of Consistency for Distributed Data (PaPoC 2019), co-located with Eurosys 2019.

Juan Caballero:

5. 40th IEEE Symposium on Security & Privacy (IEEE S&P 2019).
6. 2019 Network and Distributed System Security Symposium (NDSS 2019).

Manuel Carro:

7. 35th International Conference on Logic Programming (ICLP 2019).
8. 21st International Symposium on Practical Applications of Declarative Languages (PADL 2019).
9. 19th National Workshop on Programming Languages (PROLE 2019).
10. 29th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR 2019).

Antonio Faonio:

11. Financial Cryptography and Data Security - 23st International Conference, (FC 2019).

Dario Fiore:

12. 26th ACM Conference on Computer and Communications Security (ACM CCS 2019).
13. 22nd International Conference on Practice and Theory of Public-Key Cryptography (PKC 2019).



John Gallagher:

- 14. 35th International Conference on Logic Programming (ICLP 2019).
- 15. 7th International Workshop on Verification and Program Transformation (VPT 2019).
- 16. 6th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2019).
- 17. ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation (PEPM 2019).

Pierre Ganty:

- 18. 17th International Symposium on Automated Technology for Verification and Analysis (ATVA 2019).
- 19. 23rd International Conference on Developments in Language Theory (DLT 2019).
- 20. 25th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2019).

Alvaro García:

- 21. 39th IEEE International Conference on Distributed Computing Systems (ICDCS 2019).

Alessandra Gorla:

- 22. 35th IEEE International Conference on Software Maintenance and Evolution (ICSME 2019).

Alexey Gotsman:

- 23. 49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2019).
- 24. The 30th International Conference on Concurrency Theory (CONCUR 2019).
- 25. European Symposium on Programming (ESOP 2019).
- 26. European Conference on Object-Oriented Programming (ECOOP 2019).

Manuel Hermenegildo:

- 27. 36th International Conference on Logic Programming (ICLP 2019).

- 28. 21st ACM International Symposium on Principles and Practice of Programming Languages (PPDP 2019).

Bishoksan Kafle:

- 29. 6th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2019).

Fernando Macías:

- 30. 6th International Workshop on Multi-Level Modelling (MULTI 2019).

César Sánchez:

- 31. 19th International Conference on Runtime Verification (RV'19).
- 32. 17th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'19).
- 33. 17th International Conference on Software Engineering and Formal Methods (SEFM'19).
- 34. 39th International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2019).
- 35. 15th International Conference on integrated Formal Methods (iFM'19).
- 36. 1st International Workshop on Governing Adaptive and Unplanned Systems of Systems (GAUSS'19).

Pedro Valero:

- 37. International Symposium on Automated Technology for Verification and Analysis (ATVA 2019), Artifact Evaluation Committee Member.

Niki Vazou:

- 38. 46th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2019).



Association and Organization Committees

Manuel Carro:

1. Representative of IMDEA Software in Informatics Europe.
2. Member of the joint board of the Erasmus Mundos European Master in Software Engineering.
3. Representative of IMDEA Software in the Node Strategy Committee of EIT Digital Spain.
4. Representative of IMDEA Software at the General Assembly of EIT Digital.
5. Member of the Technical and Scientific Advisory Board of Origen Ventures Fund.
6. Member of the evaluation committee for Galician singular research centers.

Isabel Garcia:

7. Co-organizer of *I+D+M: Mujeres en Montegancedo*, event for the International Day of Women and Girls in Science.

Manuel Hermenegildo:

8. President of the INRIA Scientific Council (Institut National de Recherche en Informatique et en Automatique, France).
9. Member of the Jury for the 2019 SCIE-Fundación BBVA National Prizes in Informatics.
10. Member of the Academia Europaea.
11. Member of the Schloss Dagstuhl Scientific Advisory Board (Germany).
12. Member of the Nomination Committee of Informatics Europe.
13. Member of the evaluation committee for Galician singular research centers.
14. Member of the External Advisory Board of the NOVA LINCS Institute (Portugal).
15. Member of the IRILL Scientific Advisory Board (French Institute for Free Software).
16. Secretary of the International Association for Logic Programming.
17. Member of the International Federation for Computational Logic (IFCoLog) Advisory Board.
18. Member of the Technical University of Madrid Consulting Council.
19. Member of the Technical University of Madrid Gallery of Distinguished Professors.



Awards

Paper Awards:

1. Patrick Cousot, *Roberto Giacobazzi*, Francesco Ranzato. AI: Abstract **Interpretation**. **POPL 2019. Distinguished paper award.**

Thesis Awards:

2. *Zsolt István*. EuroSys Roger Needham PhD Award 2019. **Honorable Mention.**
3. *Luca Nizzardo*. Cryptographic Techniques for the Security of Cloud and Blockchain Systems. **UPM extraordinary award 2017-2018 for PhD thesis.**

Other Awards:

4. *Alessandra Gorla*. International Conference on Software Maintenance and Evolution (ICSME) 2019 **Distinguished reviewer award.**



Education

While the Institute focuses on research and technology transfer, our researchers are sometimes involved in teaching courses offered by universities and other entities. The following is a list of courses where IMDEA Software researchers taught in 2019.

1. Computer Security (Master level, 4 ECTS). Master in Software and Systems (MUSS) and European Master in Software Engineering (EMSE), Universidad Politécnica de Madrid (UPM). *Juan Caballero, Ignacio Cascudo, Dario Fiore, Alessandra Gorla, Marco Guarnieri.*
2. Seminar on Performance Analysis and Modeling of Software Systems (Master level, 1.5 ECTS). Universidad Politécnica de Madrid (UPM). *Zsolt Istvan.*
3. Seminar on Building Data Processing Systems with FPGAs (Master level, 1 ECTS). Universidad Politécnica de Madrid (UPM). *Zsolt Istvan.*
4. Seminar on Advanced Functional Programming (Master level, 1.5 ECTS). Universidad Politécnica de Madrid (UPM). *Niki Vazou.*





Communication

As any research institution, the IMDEA Software Institute uses different communication strategies and channels to disseminate both general science and technology principles and, in particular, the advances made by the Institute researchers. These serve to raise the scientific and technological awareness of the general public, to showcase how the investment in research reverts in the society at large, and to present the latest discoveries and developments to the relevant stakeholders. This complements scholarly dissemination, that typically takes place via publications in journals and conferences and address peer researchers.

Among the objectives of communication we may cite:

- disseminating knowledge about science and technology,
- making society at large aware of the advances obtained through investment in science and technology,
- fostering the engagement and participation of the society in STEM-related activities,
- contributing to attracting the best talent through additional visibility of the Institute.

The communication plan of the Institute is shaped as a matrix for all communication actions carried out in the areas of public relations, content marketing, corporate identity, internal communication, dissemination channels, advertising, and corporate social responsibility.



web news



press
releases



social networks
posts



media
impacts



impressions



followers/community



409.8K



3.5K



2K



32.1K



21.2K



Dissemination events

In 2019 IMDEA Software researchers have participated in multiple events related to dissemination and the promotion of science.

Women and Girls in Science

Women in Montegancedo (February 11, 2019)

In February 2019, the IMDEA Software Institute participated once more, together with research groups from UPM's Montegancedo Campus (namely, the Cajal Blue Brain Project and the Ontology Engineering Group), in the activity "Women in Montegancedo" to celebrate and encourage the role of women in science, as a part of the International Day of Women and Girls in Science.

This was a great opportunity to bring science and research closer to young girls, to encourage STEM vocations, and make it possible for the audience to interact with young and established researchers.



CAIT



12 researchers



120 Bachelor and High School students



POLITÉCNICA



i2Tech- CAMPUS MONTEGANCEDO
Universidad Politécnica de Madrid



Science and Innovation Fair

IMDEA Stand (March 28–31, 2019)



13 IMDEA Software
researchers



15.000

The *Madrid Science and Innovation Fair* (MXCI) is an event organized by the *Fundación para el Conocimiento madri+d*, in connection with the initiative #STEMadrid, with the goal of promoting science and excellence in research in the Community of Madrid. The IMDEA Institutes participated as exhibitors, presenting several activities to showcase their research.

The presence of the IMDEA Software Institute at the Fair was an invaluable opportunity to disseminate our research, demystify computer science, and encourage STEM vocations. IMDEA Software organized several activities / workshops that were attended by a large number of young students who, judging by the interest shown and the very favorable feedback received, left the stand with a positive impression and perhaps with the seed of a scientific vocation.

Video summary



fundación para el
conocimiento
madri+d

FERIA
mxci
madrid por la ciencia y la innovación



European Researchers' Night

Crime Scene Investigation (Season 3)

(10th edition, September 27, 2019)

Residencia
de estudiantes

9 researchers

200 teenagers
and parents

In September 2019, as in previous years, the IMDEA Software Institute participated in the activities for the “European Researchers' Night”, coordinated at the Regional level by the *Fundación para el Conocimiento madri+d*. The Institute organizing the event “IMDEA-CSI: Crime Scene Investigation (Season 3)”. As in previous editions of this event, the IMDEA Institutes had the privilege of collaborating with the Spanish National Police.

IMDEA researchers and members of the Scientific Police demonstrated how research done in laboratories often finds a way to eventually assist the Police in the investigation done “out on the street”, including those made at the crime scene.

Video summary



Residencia de Estudiantes



XIX Science and Innovation Week

The Roots of Software (November 11, 2019)



3 researchers



140 high school students

On the occasion of the Madrid Science and Innovation Week, more than 150 high school students attended the activity “The Roots of Software” at the IMDEA Software Institute on November, 2019. The Science and Innovation Week is an initiative from the Comunidad de Madrid, coordinated by the *Fundación para el Conocimiento madri+d*, aimed at attracting students at all levels to STEM careers and introducing young talents to research and innovation. Research assistants at the Institute used this opportunity to present some basic concepts of several areas of Computer Science through challenges, games and videos.



Research- and Technology-Related Events

REDIMadrid Workshop (October 22, 2019)

-  Campus Móstoles URJC
-  12 researchers
-  60 from industry and academic



The Madrid high-speed network for universities and research, REDIMadrid, held its XIV workshop in October at the Móstoles Campus of the Rey Juan Carlos University (URJC).

This workshop is a meeting point where research institutions and industry exchange ideas and successful experiences on the evolution and applications of very high-speed telecommunication networks.

The lineup for the 2019 edition included speakers from REDIMadrid, URJC, Universidad Politécnica de Madrid (UPM), UNED, ADVA Optical Networking, Axians, Palo Alto, and HPE Aruba Iberia.

Video summary



REDIMadrid Technical Workshop (October 23, 2019)

An internal technical meeting was organized following the open workshop to exchange ideas about new research activities, developments focused on the network, and the extension of the network itself.



Workshop on Software Reliability for MFoC

Madrid Flight on Chip project
(November 26, 2019)

IMDEA Software

12 researchers

25 industry and academic



The MFoC project (Madrid Flight on Chip) is devoted to exploring and developing novel techniques to serve the needs of aerospace industry amidst the ongoing revolution in how satellites are built and deployed. Due to recent dramatic cost reductions in launching satellites, hardware and, especially, software now dominate the costs and time constraints these missions, and a paradigm shift in how these are developed is undergoing.

The workshop brought together experts from model-based design and testing, formal methods, software engineering, static analysis, and automated testing to discuss techniques and potential applications to critical aerospace software.



AVERTIS

Analysis, Verification and
Transformation for Declarative
Programming and Intelligent Systems
(November 29, 2019)

IMDEA Software

13 researchers

60



UNIVERSITÀ
di VERONA

In November, AVERTIS, an event dedicated to Analysis, Verification, and Transformation for Declarative Programming and Intelligent Systems, took place at the Institute.

AVERTIS was an intense and very interesting day devoted to scientific dissemination, exchange of ideas, and cross-fertilization. In total, the event had 13 exceptional speakers : Roberto Giacobazzi (U. of Verona); Patrik Cousot (Courant Institute, NYU); Andy King (U. Kent); María García de la Banda (U. Melbourne); David S. Warren (SUNY at Stony Brook); María Alpuente (U. Politécnica de Valencia); Narciso Martí Oliet (U. Complutense de Madrid); Martin Wirsing (Ludwig-Maximilians-Universität München); Veronica Dahl (Simon Fraser University); Peter Stuckey (Monash University); Mike Codish (Ben-Gurion University of the Negev); Gopal Gupta (U. of Texas at Dallas); and Ricardo V. Peña Mari (U. Complutense de Madrid).



Joyfe School students

(April 25, 2019)

Five JOYFE School students visited the IMDEA Software Institute on April 2019. They were shown the premises, introduced to how work in a research center proceeds, and taught some basic notions about software and, specifically, about algorithms as building blocks with which software engineers create the applications with which we interact daily.



Lyceé Français student

Vlad Dancau (June 17-24, 2019)



Vlad Dancau, a 15-year-old student from the Lycée Français of Madrid, made a 1-week stay at the Institute as part of a program of internships in companies. A very interesting video interview gives us insights on what he learned about research, information technologies, and the relation between mathematics and computer science.

Available here:





Comunidad
de Madrid



EUROPEAN UNION
European Structural and Investment Fund

annual report
2019
software.imdea.org



imdea **software** institute



Contact

software@imdea.org

tel. +34 91 101 22 02

fax +34 91 101 13 58

Campus de Montegancedo
28223 Pozuelo de Alarcón
Madrid, Spain