science and technology
for developing better software

imdea **software** institute

annual report

2018

www.software.imdea.org

Manuel Carro
Director, IMDEA Software Institute
April 22, 2019

foreword

The IMDEA Software Institute was created by the Madrid Regional Government under the strong belief that quality research and innovation in technology-related areas is the most successful and cost-effective way of generating knowledge, competitiveness, sustainable growth, and employment. The Institute focuses on research on the science and technology behind the creation of reliable, scalable, and secure software. The relevance of software in the global market is supported by existing data: the spending on ICT for 2017 in the EU28 area was estimated in 624M€, a 4.4% of the GDP of the same area (*D2.1 First Report on Facts and Figures*, IDC Italia srl and The Lisbon Council, March 2018), while the worldwide tendency is that of a sustained growth of an approximate annual 5% (https://www.idc.com/promo/global-ict-spending/forecast, IDC Italia srl, consulted on April 2019).

In addition, trends such as the wider application of AI and the emergence of blockchain-based technologies applied to a variety of scenarios unrelated to cryptocurrencies, continued their consolidation during 2018. As with all new technologies, their adoption is not without risk, and careful deliberation is needed to ensure that they can be safely used. These are just a couple of examples highlighting why research in ICT is as necessary as always: software-related technologies, when developed correctly, indeed have an immense potential for raising industrial competitiveness, opening whole new business areas, creating high added-value jobs, protecting our security and privacy, and improving quality of life. These are the ultimate reasons for the creation of the IMDEA Software Institute.

Today, the Institute is a vibrant, exciting reality, that has reached world-class status in its objectives of excellence in attraction of talent, research, and technology transfer. The key asset of the Institute is its people: its researchers and support staff. While this is true for

any scientific discipline, it is more so in an area where, except in certain subareas, the cost of experimentation facilities is not as high as in other sciences. In line with the observation that people are key, the Institute has continued to attract to Madrid top talent worldwide, and during 2018 it included 17 faculty (one half-time), 2 visiting and associate faculty, 16 postdoctoral researchers, 3 research programmers, 26 research assistants, 29 interns, 12 project staff, and 10 staff members, from over 20 different nationalities. Our researchers have joined the Institute after working at or obtaining their Ph.D. degrees from prestigious centers, including Stanford U., Carnegie Mellon U., U. California at San Diego, or Microsoft Research in the US, 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, 246 international researchers have visited and given talks at the Institute to date.

During 2018, Institute researchers have published 73 refereed publications in some of the top venues in the field, such as OOPSLA, ACM IMC, ACM CCS, ICLP, POPL, ESOP, CRYPTO, EUROCRYPT, IEEE S&P, CAV, ICFP, LICS, PPoPP, and ICALP, given 8 invited talks in international conferences, 45 invited seminars and lectures, chaired 6 program committees, and participated as members in 48 program committees and 24 boards of journals and conferences, in addition to being conference or program chairs of 6 conferences. The Institute has received 22 best paper awards or mentions in the last 5 years.

The Institute has also participated during 2018 in 31 funded research projects and contracts and its researchers were awarded 8 fellowships. Thirteen of these projects come from international agencies and companies, six have direct industrial funding, and eleven of them involve collaboration with companies of all sizes, both Spanish and international. These companies include, among others, ATOS, Groupalia, Intel, Merlinux, NEC, Nextel, Protocol Labs, RedBorder, Relational, Scytl, Telecom Italia, and Zemsania.

This year, the Institute adapted its role within EIT Digital due to the creation of the *EIT Digital Spain* foundation that took over the coordination of the Co-Location Center and its activities. Within this new framework, the Institute, besides being a partner of EIT Digital itself, provides hosting to the Co-Location Center. This did not change the activity of the local node, which continues with its task of building an ecosystem of innovation and entrepreneurship, with the addition of new local partners, new startups hosted at the CLC, the Master and PhD lectures on entrepreneurship that are delivered at the CLC, and the training actions on innovation, business development, and coaching.

In 2018, the Institute also reinforced its collaboration with industry in security and distributed computing, two fields of high interest for many companies these days. Contracts and agreements were signed to work on secure cloud storage and privacy in blockchain computations. These included hosting personnel of these companies that can, through the interaction with our researchers, channel the transfer of knowledge from academia to the productive fabric.

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

foreword

annual report 2018

www.software.imdea.org

editor
IMDEA Software Institute

graphic design
base 12 diseño y comunicación

D.L.
M-17357-2019

contents

contents

about us

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** **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**

62 researchers

26 PhD students

18 nationalities

The 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.

- institute IMdea water
- institute IMdea nanoscience
- institute IMdea food
- institute IMdea networks
- institute IMdea energy
- institute IMdea software
- institute IMdea materials

about us

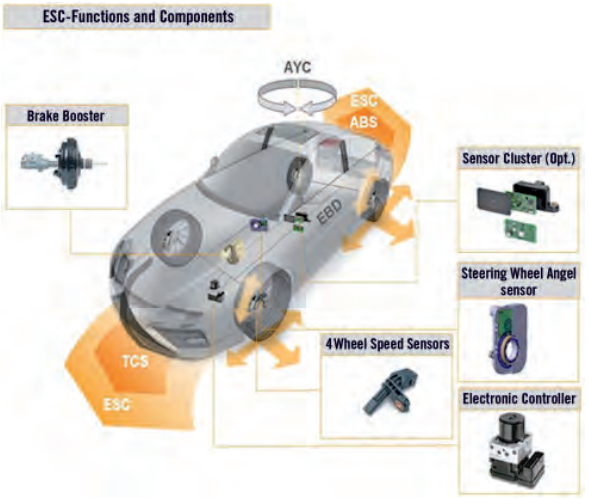
motivation and goals:

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 which, 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 more mundane devices 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 other humans. This pervasiveness explains the global figures around software: according to data from the European Commission, the overall software and software-based services (SSBS) 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 SSBS industry in Europe is expected to be 2.9% between 2015 and 2020. The 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 SSBS companies. This vividly illustrates the huge potential of the European SSBS 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 and its pervasiveness, 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). Unfortunately, developing software of an appropriate level of reliability, security, and performance, at a reasonable cost is still a challenge today. A recent study

from Cambridge University found that the global cost of debugging software has risen to $312 billion annually, while 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. 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

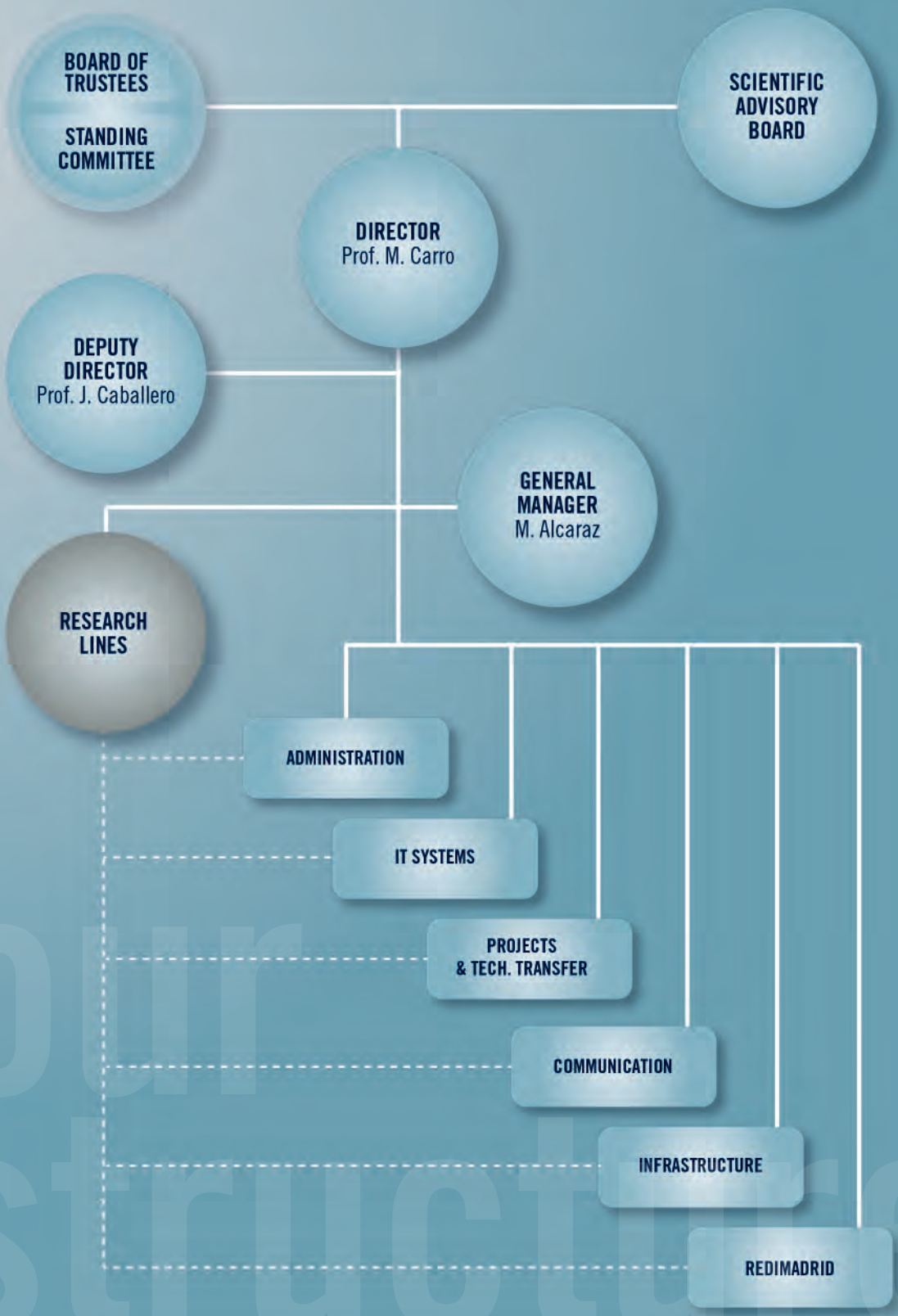
The IMDEA Software Institute is a non-profit, independent organization, constituted as a Foundation. Its structure brings together the advantages and guarantees offered by a foundation with the flexible and dynamic management typical of a private body. This combination is deemed necessary to attain the 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.

Our structure



members of the governing bodies

BOARD OF TRUSTEES

Chairman of the Foundation

PROF. DAVID S. WARREN
State University of New York at Stony Brook, USA.

Vice-chairman of the Foundation

ILMO. SR. D. RAFAEL VAN GRIEKEN SALVADOR
Councilor for Education and Research, Madrid Regional Government, Spain.

Madrid Regional Government

ILMO. SR. D. RAFAEL VAN GRIEKEN SALVADOR
Councilor for Education and Research, Madrid Regional Government, Spain.

ILMO. SR. D. ALEJANDRO ARRANZ CALVO
Director-General for Research and Innovation, Madrid Regional Government, Spain.

ILMO. SR. D. JOSÉ MANUEL TORRALBA CASTELLÓ
Director-General for Universities and Higher Art Studies, Madrid Regional Government, Spain.

ILMO. SR. D. RAFAEL GARCÍA MUÑOZ
Deputy Director-General for Research, Madrid Regional Government, Spain.

Universities and Public Research Bodies

PROF. NARCISO MARTÍ OLIET
Universidad Complutense de Madrid, Spain.

PROF. FRANCISCO JAVIER PRIETO FERNÁNDEZ
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.

Scientific Trustees

PROF. DAVID S. WARREN
State University of New York at Stony Brook, USA.
Chairman of the Board of Trustees.

PROF. PATRICK COUSOT
Courant Institute, New York University, USA.

PROF. LUÍS MONIZ PEREIRA
Universidade Nova de Lisboa, Portugal.

PROF. JOSÉ MESEGUER
University of Illinois at Urbana Champaign, USA.

PROF. ROBERTO DI COSMO
Universitè Paris Diderot and INRIA, France.

our structure

SCIENTIFIC ADVISORY BOARD

Expert Trustees

MR. JOSÉ DE LA SOTA RIUS
General Coordinator, Fundación para el Conocimiento (MadrI+D), Madrid, Spain.

MR. EDUARDO SICILIA CAVANILLAS
Escuela de Organización Industrial, Madrid, Spain.

Invited Members from Industry

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

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

Elecnor Deimos. *Mr. Ismael López, Managing Director* and *Mr. Miguel Lizondo, Information and Communication Systems Business Unit Director.*

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

Secretary

MR. ALEJANDRO BLÁZQUEZ LIDOY

PROF. DAVID S. WARREN
State University of New York at Stony Brook, USA.
Chairman of the Board.

PROF. MARÍA ALPUENTE
Universidad Politécnica de Valencia, Spain.

PROF. ROBERTO DI COSMO
Universitè Paris Diderot and INRIA, France.

PROF. PATRICK COUSOT
Courant Institute, New York University, USA

PROF. VERONICA DAHL
Simon Fraser University, Vancouver, Canada.

PROF. HERBERT KUCHEN
Universität Münster, Germany.

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.

headquarters building

Since 2013, the IMDEA Software Institute is located in its headquarters building, which was officially inaugurated in July 2013, in the Montegancedo Science and Technology Park. These premises offer an ideal environment for fulfilling the mission of attraction of talent, research, and technology transfer. They include offices, numerous spaces for interaction and collaboration, areas for project meetings and for scientific and industrial conferences and workshops, and powerful communications and computing infrastructures. 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. It is highly energy-efficient, through energy-conscious design, co-generation, and full automation.

The location of the new IMDEA Software building also provides excellent access to the UPM School of Computer Science as well as to the other research centers within the Montegancedo Science and Technology Park. These centers include the Madrid Center for Supercomputing and Visualization (CESVIMA), the Center for Computational Simulation, the UPM Montegancedo Campus company "incubator" and technology transfer center (CAIT), the Institute for Home Automation (CEDINT), the Institute for Biotechnology and Plant Genomics (CBGP), the Center for Biomedical Technology (CTB), the Microgravity Institute, and the Spanish User Support and Operations Centre for ISS payloads (USOC). In particular, the CESVIMA houses the second largest supercomputer in Spain and one of the largest in Europe, as well as a state-of-the-art visualization cave, and is equipped for massive information storage and processing, high performance computing, and advanced interactive visualization. The Institute's location also provides convenient access to the other Madrid universities and IMDEAs.

The campus obtained the prestigious "International Campus of Excellence" label, and is the only campus in Spain to receive a "Campus of Excellence in Research and Technology Transfer" award in the Information and Communications Technologies area from the Spanish government.

cooperation

Companies with which IMDEA Software Cooperated during 2018

aws
Atos
COMPARTIA
A CUSTOMER CENTRIC ORGANIZATION
eurona
ferrovial
gmv
INNOVATING SOLUTIONS
Groupalia
IBM
indra
intel
merlinux
Microsoft Research
NEC
Nextel S.A.
Ingeniería y Consultoría
NOKIA
Protocol Labs
redborder
relational
THE FINANCIAL SOLUTIONS COMPANY
Scytl
Innovating Democracy
solusoft
Tecnocom
Telefónica
Investigación y Desarrollo
TIKAL
zemsania
Tech outsourcing services

Academic Institutions with which IMDEA Software Cooperated during 2018

Other Publicly-Funded Institutions with which IMDEA Software Cooperated during 2018

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, 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 (EIT Section, pages 56-59). 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 further in Chapter Research Projects and Contracts, pages 54-73, 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., Microsoft funds research students working on software verification and security), *research stays of Institute researchers at company premises* (e.g., Institute researchers have made industrially-funded extended stays at Deimos Space, Microsoft Redmond in the US, or Microsoft Cambridge in the UK), *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.
- Roskilde University, Denmark.
- Consejo Superior de Investigaciones Científicas.
- Swiss Federal Institute of Technology (ETH) Zurich.

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.

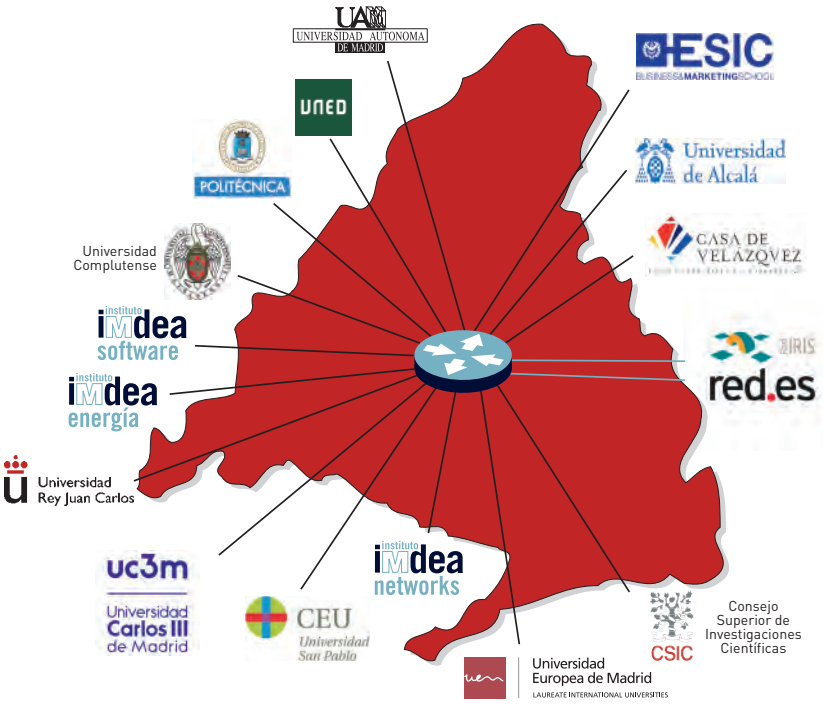
The Institute also has a strong presence in national and international bodies. It is a member of *Informatics Europe*, the organization of all deans, chairs, and directors of the leading Departments and Institutes of Computer Science in Europe. Manuel Hermenegildo, Director of the Institute until the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

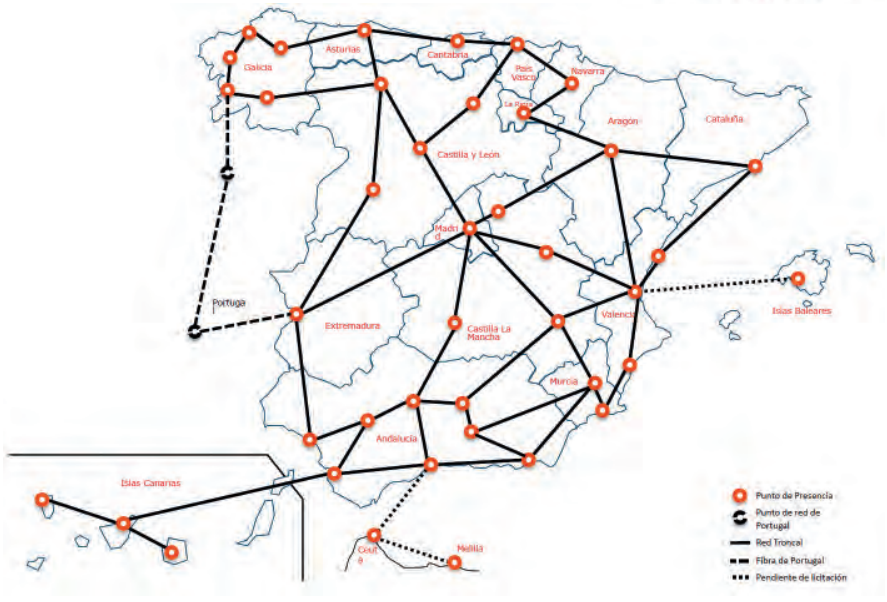
REDIMadrid

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 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 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 2018, REDIMadrid continued its expansion plan to a dark fiber network with the acquisition of links connecting both points of presence of REDIMadrid (at CIEMAT and CSIC) with the main campuses of Universidad Carlos III and Universidad Rey Juan Carlos, and with the IMDEA Networks Institute. The deployment of these links finished in 2018, and was followed by the public tender of optical and communication equipment to activate all the redundant links in the first quarter or 2019.


UAM
UNIVERSIDAD AUTONOMA DE MADRID
UNED
POLITÉCNICA
Universidad Complutense
ESIC
BUSINESS&MARKETINGSCHOOL
Universidad de Alcalá
CASA DE VELAZQUEZ
instituto imdea software
instituto imdea energía
Universidad Rey Juan Carlos
RedIRIS
red.es
uc3m
Universidad Carlos III de Madrid
CEU Universidad San Pablo
instituto imdea networks
CSIC
Consejo Superior de Investigaciones Científicas
Universidad Europea de Madrid
LAUREATE INTERNATIONAL UNIVERSITIES


RedIRIS
red.es
Galicia
Asturias
Cantabria
País Vasco
Navarra
Aragon
Cataluña
Castilla y León
Madrid
Portuga
Extremadura
Castilla La Mancha
Valencia
Islas Baleares
Murcia
Andalucía
Islas Canarias
Ceuta
Melilla
Punto de Presencia
Punto de red de Portugal
Red Troncal
Fibra de Portugal
Pendiente de licitación

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 correctness of a program is essential in many existing and emerging industrial domains where a program malfunction 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 worldwide 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 efficent deductive methods for software verification

- Sofware 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.

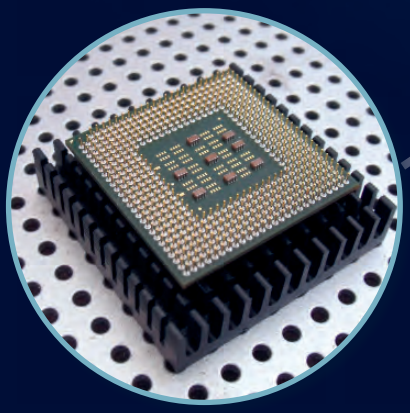
Side-channel attacks and countermeasures

- 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

Madrid Flight on Chip

Verification with Liquid Types



Narrowing the Data/Compute Gap with Specialized Hardware

Madrid Flight on Chip

The project Madrid Flight on Chip (MFoC) is a research and innovation project funded by Comunidad de Madrid.

The goal of the MFoC project is to develop novel techniques for the development of future-generation aerospace satellite systems. The project will explore hardware and software techniques for radically different aerospace system development in that will enable much more cost-effective satellite missions with lower development time possible with new-generation System-on-Chip designs, while maintaining high levels of reliability.

The project will explore the use of modern hardware architectures, including FPGAs and commercial multi-core to solve common problems in the target aerospace application domain. These problems include energy consumption and resistance to cosmic radiation. The software techniques will include applications of software engineering techniques like model-based design and automated code generation and testing.

The role of the IMDEA Software Institute in the MFoC project will be the research, adaptation, and technology transfer of techniques from program analysis, runtime verification, and automated test generation to the verification and validation phase of aerospace software development. Due to the demand for high-reliability of satellite systems, the development of their software is very slow and costly. In turn, as projects become more complex, verification and validation, usually relying on highly manual techniques, dominate time and overall cost. In this project, the IMDEA Software Institute will explore formal and semiformal techniques to improve the state-of-the-art of verification and validation of the new-generation satellite systems.

To improve the chances of success, the project will exploit specific characteristics of the on-board software developed for satellite missions. This software is to follow very strict coding rules and patterns. One of the main challenges will be to tackle automatically generated code produced using model-based development technologies.

The MFoC consortium includes SENER as the main aerospace industrial partner and IMDEA Software and Universidad Carlos III as research partners, with GENERA, CENTUM, REUSE and MARM being the rest of the industrial partners.

Usable and Useful Verification with Liquid Types

The goal of verification is to formally prove the absence of bugs in software, and it has attracted increased attention, since software bugs have, in the past, cost time, money, and even human lives. However, up to now, formal verification has been decoupled from mainstream software development. The liquid types line of research aims to strongly couple software development and formal verification in a way that is both efficient and easily accessible to developers so that software bugs are detected early in the development pipeline.

Refinement types make formal verification accessible to mainstream software developers by extending existing programming languages to also act as automated and usable verifiers. Having realized the importance of formal verification, both academia and industry are spending a large amount of resources to ensure software correctness. Yet, up to now, software development and formal verification are separated, requiring verification experts to prove properties of template implementations ported to verification-specific languages (like Coq, Agda, etc).

Liquid Haskell is a refinement type checker that extends the general-purpose programming language Haskell with full theorem proving capabilities, so that users of Haskell can formally verify properties of their programs. Liquid Haskell takes as input real-world Haskell source code, annotated with correctness specifications in the form of refinement types, and checks whether the code satisfies the specifications. Liquid Haskell has been accepted by both academic and industrial Haskell users as a usable verifier, since it allows for natural integration of expressive specifications and automatic verification, and is used in real world applications. Up to now, it has been used to verify decidable properties that include inbounds list and memory indexing, and datatype invariants such as sortedness and uniqueness. Recently, Liquid Haskell has been extended to a fully expressive theorem prover that is semi-automated by an SMT solver over decidable logics. Using this extension, it has been used to verify sophisticated program properties, like equivalence of program optimizations, noninterference, and resource requirements.

Liquid Haskell is a very successful experiment in which formal verification became an integral part of the development environment of a general-purpose language, Haskell, to create both correct and efficient software systems. The lessons learnt from this experiment can be adapted to mainstream languages such as Ruby and JavaScript, for which today verification is challenging and, due to their widespread usage, crucial.

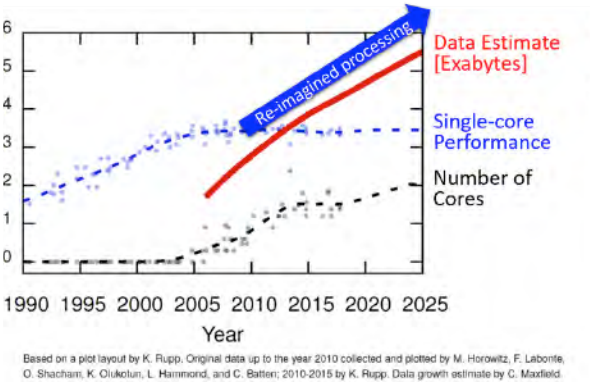
Narrowing the Data/Compute Gap with Specialized Hardware

Datacenters are facing a challenge because the quantity of information that needs to be stored and processed is growing faster than the performance of general purpose processors. For decades, this has been increasing as per Moore's Law, but today it is unclear whether the trend can be maintained. The shrinking of transistor sizes has slowed down significantly and even though it is possible to add more transistors to a central processing unit (CPU), using them to create additional cores is unlikely to benefit applications unless they are trivially parallelizable.

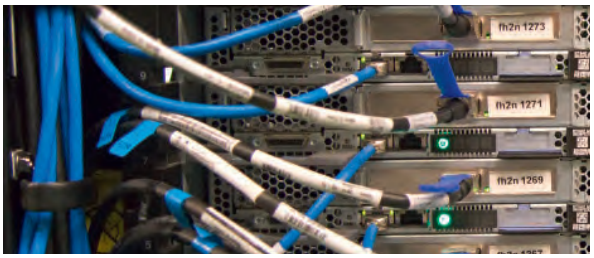
In order to change the status quo, we need to investigate how software interacts with the underlying hardware and explore ways in which we could tailor the latter to the application's needs. As an alternative to adding conventional cores, we could use part of the chip for specialized processing elements. When tailored to widely-used application domains in datacenters, these elements increase overall processing efficiency and could be used to narrow the gap between data growth and compute capacity.

There are already several types of programmable hardware devices appearing in the datacenter and consumer clouds, which makes this an exciting time to be working in the field of systems. Emerging low latency networks with programmable network interface cards, for instance, allow distributed applications to change their communication model and various types of programmable hardware accelerators allow compute-intensive tasks to be carried out faster or in a more energy efficient manner. The shift away from a "CPU-only" view, however, requires us to devise better methods for software to take advantage of, or even to directly drive the design of, novel hardware features.

At our institute, we explore research questions related to integrating programmable hardware accelerators in data management systems that suffer from various forms of data movement bottlenecks (e.g., large-scale distributed databases, blockchains, etc.) and emerging distributed data-intensive applications that are often bound by the processing power of CPUs (e.g., business analytics, machine learning, etc.) The most important challenges of this research direction revolve around the goal of ensuring that, while we benefit from the use of novel hardware, the flexibility, reliability, as well as the security guarantees, of applications are not impacted. In our exploration we employ rigorous analysis methods, build proof of concept software systems and even prototype specialized functionality in hardware, using Field Programmable Gate Arrays (FPGAs).



Stagnating CPU performance (approximated here by single-core frequency) is limiting our ability to process the increasing amounts of data we produce. Using more specialized hardware is one promising direction to close the gap between data and computation.

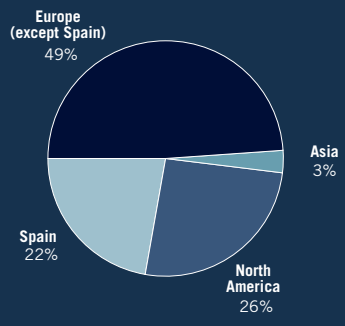


people

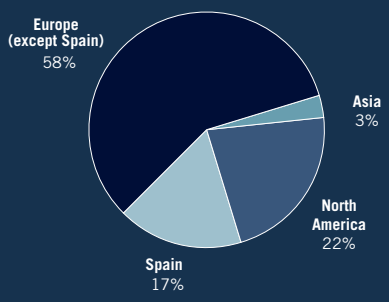
The IMDEA Software Institute strives towards the level of excellence and competitiveness of the highest-ranked institutions worldwide. Success in this goal can only be achieved by **recruiting highly-skilled personnel** for the scientific teams and support staff. The Institute considers this one of the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

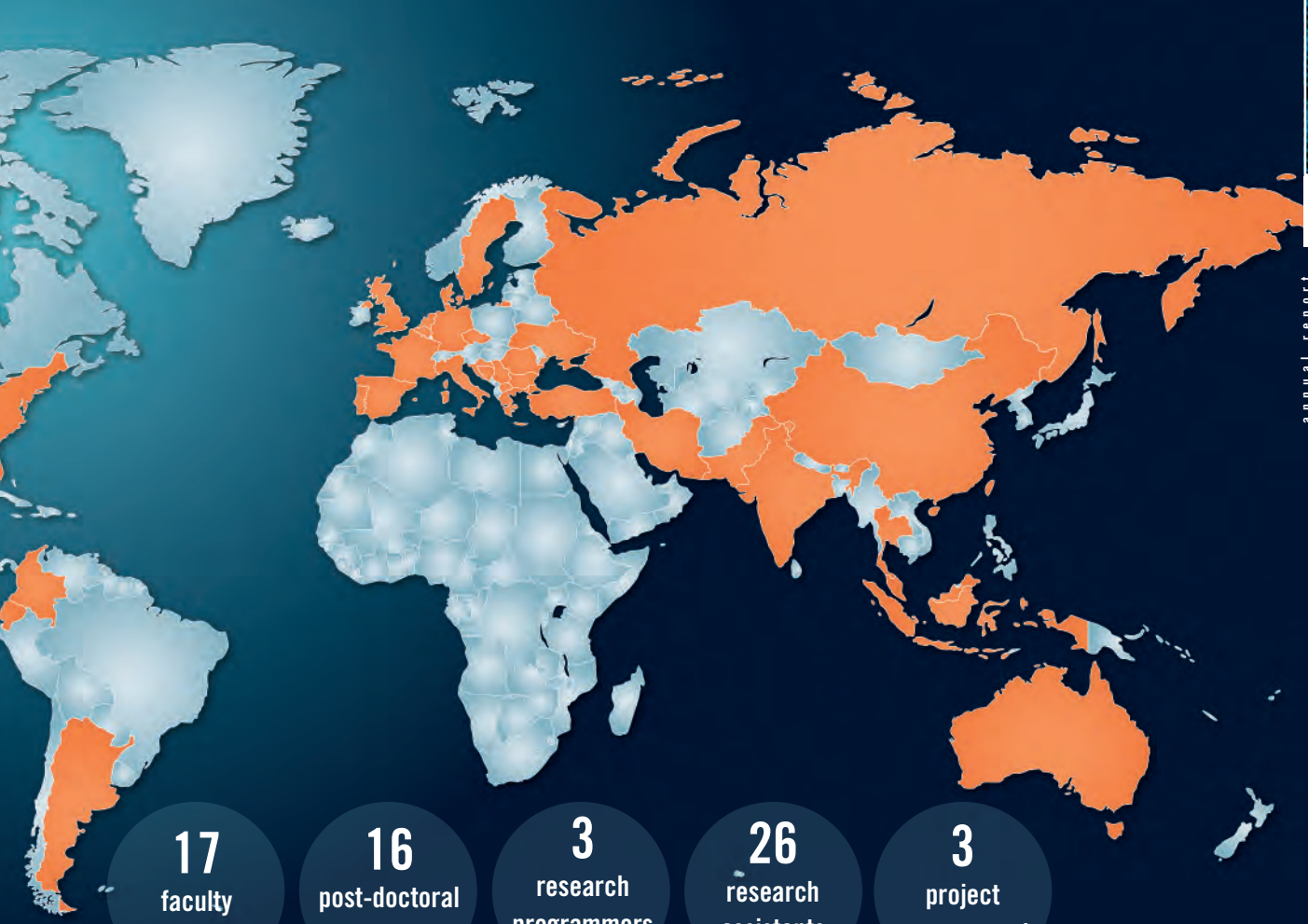
Hiring at the Institute follows **internationally-standard open dissemination procedures with public, international** calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and 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 (https://ec.europa.eu/), which it has duly signed.



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



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



17 faculty members

16 post-doctoral researchers

3 research programmers

26 research assistants

3 project management

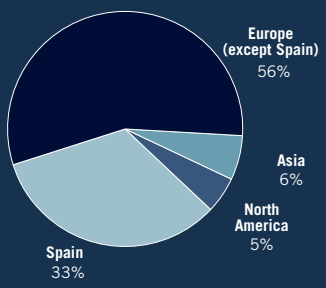
8 EIT Digital project staff

3 IT staff

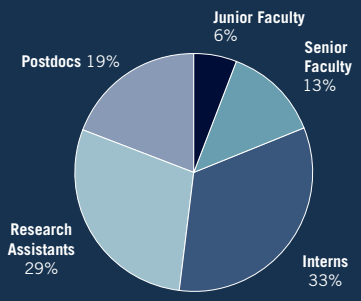
3 REDIMadrid

4 administrative support

1 communication



Nationality of researchers at or above postdoc level (by continent + Spain)



Type of position, all researchers

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 four Ph.D. theses and is supervising another one.

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 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 is an Associate Editor for the ACM Transactions on Privacy and Security (TOPS) journal and a member of the steering committee for the DIMVA, ESSOS, and JNIC conferences. He has been program chair or co-chair for ACSAC, DIMVA, DFRWS, ESSOS, and EuroSec. He has been a member of the technical committee for the top computer security venues including IEEE S&P, ACM CCS, USENIX Security, NDSS, WWW, RAID, AsiaCCS, and DIMVA.

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 and targeted attacks 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 a 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 scientific 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

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.

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.

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 International 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 become 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 that he obtained late 2007. After his Ph.D., Pierre did a nearly two-year postdoc at the University of California, Los Angeles. Pierre joined the IMDEA Software institute in the Fall 2009 as a tenure-track assistant research professor. He was granted tenure and promoted to associate research professor in December 2015. Currently he is supervising two Ph.D. students.

Research Interests

Pierre is interested in automated verification whose goal is to prove the absence of errors in idealized models of computing systems in a fully automated way. Pierre focuses on models with infinitely many states which naturally arise when control or data is unbounded. He is also interested in formal language theory and its applications to practical problems like searching text stored in compressed form. Pierre's contributions range from theoretical results all the way down to implementation of analysis algorithms.

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' research focus is on developing type-theoretic ideas on how we should develop and structure mathematical proofs about properties of programs, especially 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. Prior to his Ph.D., Alexey did his undergraduate and master studies in Applied Mathematics at Dnepropetrovsk National University, Ukraine, interning at the University of Trento, Italy, in the process. He is a recipient of a Ramón y Cajal fellowship, and an ERC Starting Grant in 2016.

Research Interests

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

Boris Köpf

Associate Research Professor

Boris joined the IMDEA Software Institute in 2010 after completing a Ph.D. in the Information Security group of ETH Zurich and working as a postdoc at the Max Planck Institute for Software Systems. Before that, he studied mathematics at the Universidad de Chile, the Universidade Federal de Campinas, and the University of Konstanz, from which he received an M.Sc. He is an alumnus of the German National Academic Foundation, holds a Ramón y Cajal fellowship, and is leading a Spanish national project (DEDETIS).

Research Interests

Boris is working on principled techniques for reasoning about security/performance tradeoffs in software systems. The goal of his work is to provide engineers with practical tools to tap unexplored performance potentials while retaining adequate degrees of security.

Dario Fiore

Assistant 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 Incorporacíon 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 was an invited speaker at research and industrial conferences including Zurihac 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 automatic light verification of Haskell code (e.g., bound checking) to sophisticated theorem proving (e.g., non-interference).

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 60 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.

postdoctoral researchers

Research Interests

In the past his research interests were related with different areas like: meta-heuristic optimization and code parallelization for the exploitation of heterogeneous computer architectures like HPC and embedded platforms. Now at IMDEA Software Institute he is applying his previous experience to work on automatic transformation of programs for tackling the complexity of efficiently programming heterogeneous platforms.

Guillermo Vigueras

Postdoctoral Researcher

Guillermo Vigueras joined IMDEA Software Institute as a postdoctoral researcher in November 2013. He received his Ph.D. degree in Computer Science from University of Valencia (Spain). During his Ph.D. he did several internships at different European institutions and research groups like the Distributed Systems and Middleware Group at INRIA-Rennes, under the supervision of Thierry Priol. Before joining IMDEA, he worked as a postdoctoral researcher at the Biomedical Engineering Department of King's College London (KCL) and the IMDEA Materials Institute, where he worked within multidisciplinary teams for computer simulation of different scientific and engineering problems. During his stay at KCL he developed the first GPU implementation of human cardiac electromechanical models for assisting in patient specific diagnosis.

Research Interests

Vincent is interested in automatic analysis of programs and in the formal verification of such analyses on semantic grounds. More specifically, he focuses on the automatic proof of program equivalence using product programs, the analysis of smart contracts from the Ethereum block-chain, and the compilation of C programs to circuits to use them in cryptographic protocols. Most of the analyses he implements are formally verified using the Coq proof assistant.

Vincent Laporte

Postdoctoral Researcher

Vincent Laporte joined the IMDEA Software Institute as a post-doctoral researcher in January 2016. He received his Ph.D. in Computer Science from the University Rennes 1, France, in 2015, under the supervision of Sandrine Blazy and David Pichardie. During his Ph.D., he contributed to the implementation and the formal verification of the Verasco static analyzer.

Álvaro García Pérez

Postdoctoral Researcher

Álvaro García Pérez received is 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. During his Ph.D., he has contributed to the study of abstract machines and lambda calculi with explicit substitutions. He has also developed semantic models for call-by-value programming languages. While in Reykjavik University, his focus was on meta-theory of structural operational semantics, where he has applied nominal set theory to develop rule formats for process calculi with binding constructs. Lately, he has contributed to the verification of consensus protocols in the family of the Paxos algorithm, and he is currently working in Byzantine protocols, federated voting, and other aspects related to blockchain technology.

Antonio Faonio

Postdoctoral Researcher

Antonio received his Ph.D. degree in Computer Science from Sapienza University of Rome, Italy, where he was adviced 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 cryptography, tamper-resilient cryptography, theory of interactive proving systems, non-malleability and controlled-malleability, re-randomizable cryptosystems and verifiable mixing networks, and subversion resilient cryptography.

Wouter Lueks

Postdoctoral Researcher

Wouter Lueks received his Bachelor and Master's degrees in Mathematics and Computing Science from the University of Groningen, The Netherlands. In 2017, he received a Ph.D. degree in Computer Science from the Radboud University, Nijmegen, The Netherlands where he was advised by Bart Jacobs and Jaap-Henk Hoepman. Starting 2017, Wouter is a postdoctoral researcher at the IMDEA Software Institute working on privacy-enhancing technologies advised by Carmela Troncoso.

Research Interests

Wouter's research interests are privacy and security. He is interested in building secure, practical, and privacy-friendly systems using applied cryptography and statistical techniques.

Ignacio Fábregas

Postdoctoral Researcher

Ignacio Fábregas received both his bachelor degree in Mathematics and Ph.D. in Computer Science at 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 joined the IMDEA Software Institute as a postdoctoral researcher in May 2017. Prior to taking up this position, Avinash was pursuing his Ph.D. in Information and Communication Technology from University of Trento, Italy, where he graduated in April 2017. During his Ph.D., he worked as an Early-Stage Researcher at the Fondazione Bruno Kessler, Italy. He also spent 18 months of his Ph.D. at SAP Labs France, working closely with the product security research team of SAP. Avinash pursued his Bachelors in Computer Science and Engineering (graduated in 2011) and Masters in Cyber Security (graduated in 2013) 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 has led to the discovery of hundreds of serious security vulnerabilities in prominent web sites. Recently he also started focusing on the automatic detection of potentially unwanted programs and malware.

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.

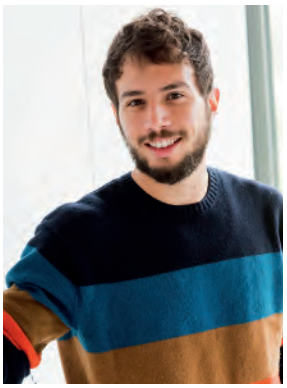
Srdjan Matic

Postdoctoral Researcher

Srdjan Matic obtained a B.Sc. and an M.Sc. in computer science from the Universita degli Studi di Milano. During his Ph.D. at the Universita degli Studi di Milano, he spent half of his time as a visiting student at the IMDEA Software Institute. He is a postdoctoral researcher at IMDEA Since June 2017.

Research Interests

Srdjan' research main line of research includes privacy and security issues that affect systems and their users. In the past he studied leaks of sensitive information in public cloud services and topological relations among hosts of spamming infrastructures. During his Ph.D. he focused on anonymity networks and specifically on threats to owners of different services that are available in the Tor network.



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.

Serdar Erbatur

Postdoctoral Researcher

Serdar joined the IMDEA Software Institute as a postdoctoral researcher in January 2018. He received his Ph.D. in Computer Science from University at Albany (SUNY) in 2012. During his PhD, he worked on unification theory which aims at solving equations in a general way, and focused on applications to cryptographic protocol analysis. He held postdoc positions at University of Verona (Italy) and LMU Munich (Germany), and visited INRIA Nancy (France) and Technical University of Valencia (Spain) for short terms.

Research Interests

Serdar's research in different research fields, including automated reasoning and type-based program analysis, has an overarching goal: applications to formal verification (of programs and protocols). He has two ongoing research projects; (i) knowledge problems for protocol analysis and (ii) the GuideForce project in which he develops a program analysis tool for checking if a given Java program follows a desired best programming practice (guideline).

Marco Guarnieri
Postdoctoral Researcher

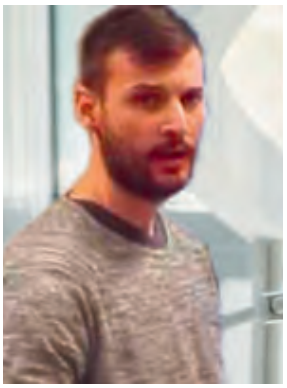
Marco joined the IMDEA Software Institute as a postdoctoral researcher in July 2018. Before that, he worked as a postdoctoral researcher at ETH Zurich, where he also completed a Ph.D. in the Information Security group. He received his bachelor's and master's degrees in computer engineering from Università degli Studi di Bergamo. During his bachelor studies, he did an internship at SAP Labs France.

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.

Joseph Izraelevitz
Postdoctoral Researcher

Dr. Joseph (Joe) Izraelevitz joined IMDEA Software Institute as a postdoctoral researcher in January 2018. He previously defended his doctoral degree in December 2017 under Prof. Michael L. Scott at the University of Rochester in Rochester, NY. He received his undergraduate degree from Washington University in St. Louis in 2009.

Research Interests
Joe's research interests include distributed computing theory, shared memory synchronization, and parallelism in general. With a background in shared memory programming, his doctoral research explored the impact of new non-volatile memory technologies on both practical systems infrastructure and formal program reasoning.



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.

research
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

Roberto Giacobazzi
Affiliate Faculty

Anindya Banerjee
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, and also at Universidad Complutense de Madrid (UCM).

Miriam García
Research Assistant

Degree: M.Sc. in Mathematical Modeling in Engineering, University of L'Aquila and University of Hamburg.

Research: Stability analysis based on model-checking techniques; hybrid systems; applied mathematics (PDEs, dynamical systems).

Artem Khyzha
Research Assistant

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

Research: Artem is interested in providing mathematical tools for understanding and proving correctness of concurrent algorithms operating on shared memory. His research efforts have focused on designing techniques for proving linearizability of non-blocking algorithms and data structures, and formalising those techniques in program logics.

Nataliia Stulova
Research Assistant

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

Research: Assertion languages, their design and use in automatic program documentation, source code specification and instrumentation. Assertion-based run-time software verification and debugging. Combination of static and dynamic program analysis.

Maximiliano Klemen
Research Assistant

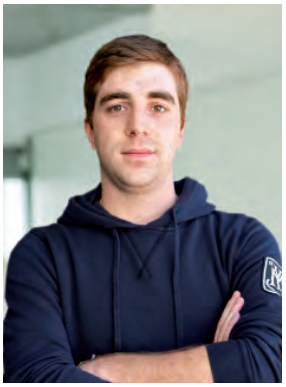
Degree: B.Sc., Universidad Nacional del Comahue (UNCo), Argentina.

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 and tabling, and their application to reasoning over stream data and abstract interpretation.



Luca Nizzardo
Research Assistant

Degree: M.Sc. in Mathematics, Università degli Studi di Milano-Bicocca, Italy.

Research: Cryptography and its applications to cloud computing security, homomorphic signatures.

Miguel Ambrona
Research Assistant

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

Research: Computer-aided cryptography with particular emphasis on automatic proofs in the generic group model, improvements on attribute-based encryption and indifferentiability analysis.

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 guaranties for cache algorithms. I focus on modeling the cache architecture, the cache algorithms and the possible side channel attacks in order to obtain security guaranties 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 Gutiérrez
Research Assistant

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

Research: Formal program verification using Horn clauses: linearisation of constraint logic programs. Applications of automata theory for solving problems in formal languages.

Pedro Valero
Research Assistant

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

Research: Applications of language's theory into data validation.

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.

Richard Rivera
Research Assistant

Degree: M.Sc. in Software and Systems, Technical University of Madrid (UPM), Spain, and Engineering in Information Systems and Computing, Escuela Politécnica Nacional (EPN), Ecuador.

Research: Malware analysis and classification, cybercrime, machine learning applied to security, development and optimization of malware analysis environments.

Umer Liqat
Research Assistant

Degree: M.Sc. in Computational Logic, Technical University of Madrid (UPM) and Dresden University of Technology (TUD), Germany.

Research: Static resource analysis and verification of non-functional program properties (execution time, energy, etc.) and its applications to Energy-aware software engineering, transformation-based analysis framework for multi-language analysis and optimizations trading-off precision/performance/energy.

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: Asymmetric and symmetric cryptography, privacy in cloud systems, cryptocurrencies and blockchain technology, electronic voting, post-quantum security.

Silvia Sebastián
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 Domínguez
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.

Interns

Intern	Period	Nationality
Chana Weil-Kennedy	03/18-07/18	France
Juan Diego Campo	01/18-12/18	Uruguay
Soheil Khodayari	10/18-12/18	Iran
Gibran Gómez	02/18-07/18	Mexico
Manuel Valbuena	07/18-12/18	Spain
Matias Spatz	04/18-04/18	Spain
David Lilue	01/18-01/18	Venezuela
José Luis Castañón	02/18-07/18	Spain
Sergio Valverde	02/17-09/18	Spain
Paloma Pedregal	03/18-10/18	Spain
Guillermo Paredes	03/18-12/18	Spain
Daniel Domínguez	03/18-10/18	Spain
Roberto Fernández	09/17-12/18	Spain
Than Hai Tran	10/18-12/18	Vietnam
Anatole Lefort	03/18-08/18	France
Luis Miguel Danielsson	05/17-12/18	Spain
Ignacio de Casso	04/18-12/18	Spain
Jose Carlos Garde	03/18-07/18	Spain
Jorge Blázquez	04/18-12/18	Spain
Borja de Regil	10/16-12/18	Spain
David Pérez	06/18-08/18	Spain
Álvaro Feal	07/17-01/18	Spain
Arianna Blasi	03/17-02/18	Italy
Fedor Ryabinin	10/18-12/18	Russia
Dimitris Kolonelos	09/18-12/18	Greece
Andrés Sánchez	09/18-12/18	Spain
Eva García	10/18-12/18	Spain
Ankita Sadu	12/18-12/18	India
Lucas Kuhring	10/18-12/18	Germany

transfer staff
project and technology

Project Staff provide additional support for the development of projects and contracts being carried out at the Institute. They are typically co-funded by such projects.

Juan José Collazo
Project Manager

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

Silvia Díaz-Plaza
Project Assistant, N-GREENS (on leave)

Degree: B.Sc. in Administration and Business Management, Universidad Rey Juan Carlos, Madrid, Spain.

Teresa Giménez
Project Assistant, N-GREENS

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

Jesús Contreras
EIT Digital Spain Node Correspondent

Degree: MBA – CEREM and Ph.D. in CS, Technical University of Madrid (UPM), Spain.

Francisco Ibáñez
Business Developer, EIT Digital

Degree: MBA Finance & Entrepreneurial Management, Harvard Business School, USA.

Susana Negrete
Doctoral Training Center Lead, EIT Digital

Degree: Ph.D. in Fungal Genetics and Genetic Engineering, Imperial College, London.

Javier Benito
Business Development Accelerator EIT Digital

Degree: MBA, ESEUNE & Ph.D. in Industrial Organization Engineering, University of the Basque Country, Spain.

Pedro Sánchez
Business Development Accelerator EIT Digital

Degree: Technical Degree, Mechanics and Industrial Automation, Lycée technologique du Rempart, Marseille, France.

Carlos Rubal
Business Development Accelerator EIT Digital

Degree: M.Sc. in Management, Northwestern University, USA.

Álvaro de la Cruz
Social Media & Web Manager – EIT Digital

Degree: BA in Political Science, UCM, Spain, Certificate of European Policy Studies, Sciences Po Strasbourg, France.

Andrea Iannetta
Administrative Assistant, EIT Digital

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

Begoña Moreno
Management Support (part time)

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

technical support and infrastructures unit

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

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

REDIMadrid staff

David Rincón
REDIMadrid Network Engineer

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

Carlos Ricardo de Higes
REDIMadrid Technician and Computer Operations

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

Carlota Gil
Accounting Assistant

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

management
& administration

María Alcaraz
General Manager

Degree: MBA – Escuela Internacional de Negocios, CEREM, Madrid, Spain

Paola Huerta
Human Resources Assistant
(part-time)

Degree: M.A. in Art History, Universidad Complutense, Madrid, Spain

Lídice González
Administrative Assistant

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

Tania Rodríguez
Administrative Assistant
(part-time)

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

communication

Blanca Gutiérrez
Communication Manager

Degree: MS in Corporate Communication Management – EAE, OBS and University of Barcelona, Spain

research projects and contracts

research projects and contracts

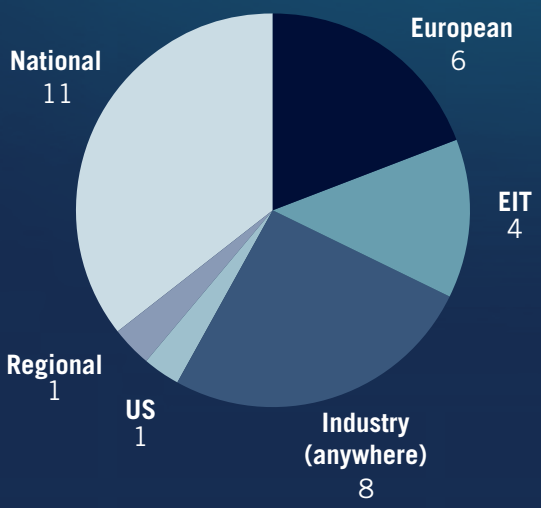


Figure 1. Projects by origin of funding

An important source of funding and technology transfer opportunities for the Institute are cooperative projects, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. During 2018, the Institute participated in a total of 31 funded research projects and contracts, many of which (13, a 41%) involve collaboration with industry and eight of them have direct industrial funding. Of these 31 projects, 15 come from international sources (11 funded by the European Union, one by the ONR-US agency, and four by foreign companies), 13 have a national source, and funds for three come from regional sources, either through competitive calls or via contracts with companies. Note that due to non-disclosure agreements not all the industrial projects them are reported in the rest of this chapter. Figure 1 shows the origin of project funding. In the same year, the Institute benefited from 8 fellowships.

The trend of external funding for the period 2012-2018 is shown in Figure 2. The amount of external funding for 2018 amounts to €2.6M, with the percentage of external funding for research and innovation w.r.t. the total Institute budget reaching 46%.

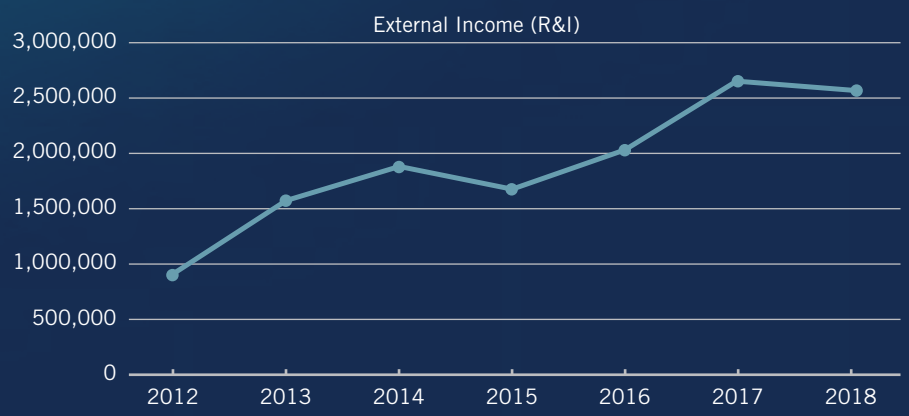


Figure 2. Evolution in external funding since 2012

Projects Running in 2018

EIT Digital

Action lines


eit Digital
EIT Digital is supported by the EIT, a body of the European Union
Helsinki
Stockholm
Berlin
Eindhoven
London
Paris
Budapest
Trento
Madrid

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 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, 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).

One of the key goals of IMDEA Software as initial Spanish Associate Member was to promote, motivate, and organize the presence of EIT Digital in Spain, and to foster 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. The opening ceremony for the new node was held on March 2, 2017, with the attendance of, among others, Mr. Tibor Navracsics, Commissioner for Education, Culture, Youth and Sport, Mr. Íñigo Méndez de Vigo, Spanish Minister for Education, Culture, and Sport, and Spokesperson of the Government, and Mr. Willem Jonker, CEO of EIT Digital. Becoming a Full Node enabled a faster expansion of activities, as is demonstrated by the fact that €15 million were invested in 2017 alone in Spanish Innovation & Entrepreneurship, as well as Entrepreuneurial Education activities.

During 2017 and 2018, the Madrid node was expanded to include Ferrovial, Nokia Spain, Ferrovial Agromán, Innovalia, Centro de Innovación de Infraestructuras Inteligentes / CI3. The partners at the Madrid node participated in 20 activities during 2018, of which 9 where innovation activities and the rest were either structural or related to education and training. In total, the budget for all of these activities was €3.4M and the budget for the innovation activities was €2.8M. That budget brought a net contribution for the Spanish partners of €2.6M, of which €2.1M correspond to innovation activities.

The transition of the management of the Spanish node from IMDEA Software to an independent foundation (EIT Digital Spain) marked a change in the role of IMDEA Software in EIT Digital. While formerly IMDEA Software was the employer of all of

EIT Digital Spain staff, during 2018 they were successively transferred to EIT Digital Spain, so that at the beginning of 2019, none of the EIT Digital Spain employees were in IMDEA Software.

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 (and will continue 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) at the disposal of EIT Digital Spain. On top of that, the Institute continues submitting innovation activities to EIT Digital.

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. In 2018 the business acceleration activities of the Madrid Node were consolidated even more, establishing relationships with the Spanish corporate and entrepreneurship ecosystem.

EIT Digital Higher Education Schools

During 2018, the Spanish Node expanded 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.

SynCrypt

Automated Synthesis of Cryptographic Constructions

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2015-2018
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.

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.

N-GREENS

Next-Generation Energy-Efficient Secure Software

Funding: Regional Government of Madrid
Duration: 2014–2018
Project Coordinator: Res. Prof. Gilles Barthe

The N-GREENS Project addresses the ever-growing economic and strategic significance of the software industry, the presence and ubiquity of software and computer devices in everyday life, and the resulting need for revolutionary solutions to enable citizens to access myriads of such services in a secure and sustainable way. Along with a strong research component carried out by a world-class expert consortium, the project has a strong technology transfer component. N-GREENS aims at developing disruptive technologies in some of the key areas with a high social impact. Its technical areas include: green computation, cloud security, cyberphysical systems, parallelism for the masses, and the resulting software tools.

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

e-TUR2020

e-TUR2020. TUrismo & Retail

Funding: Spanish Ministry of Economy, Industry, and Competitiveness – CDTI
Duration: 2015-2019
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, Eurona, Groupalia, SoluSoft, Tecnocom, 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.

ARVI

Runtime Verification Beyond Monitoring

Funding: European Union, COST Action
Duration: 2014–2018
Investigator: Assoc. Res. Prof. César Sánchez

Runtime verification (RV) is a computing analysis paradigm based on observing a system at runtime to check its expected behavior. RV has emerged in recent years as a practical application of formal verification, and a less ad-hoc approach to conventional testing by building monitors from formal specifications. There is a great potential applicability of RV beyond software reliability, if one allows monitors to interact back with the observed system, and generalizes to new domains beyond computer programs (like hardware, devices, cloud computing, and even human-centric systems). Given the European leadership in computer-based industries, novel applications of RV to these areas can have an enormous impact in terms of the new class of designs enabled and their reliability and cost-effectiveness.

CryptoAction

Cryptography for Secure Digital Interaction

Funding: European Union, COST Action
Duration: 2014–2018
Investigator: Asst. Res. Prof. Dario Fiore

As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount. Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communications: recent breakthroughs in cryptography enable the protection – at least from a theoretical point of view – of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc. However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with "the big picture". Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas produced in Europe's many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed. The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

EUIN Grants

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2017 – 2018

Europa Investigación Grants, funded by MINECO, support the submission of proposals from Spanish research groups to calls belonging to the H2020 Framework Programme. IMDEA Software has obtained two of these grants to support the submission of two research proposals to the European Research Council (for Starting Grant, made by Dario Fiore, and Advanced Grant, made by Roberto Giacobazzi) in 2017.

NEXTLEAP

NEXt Generation Technosocial and Legal Encryption Access and Privacy

Funding: European Union – H2020 Framework Program
Duration: 2016-2018
Principal Investigators: Asst. Res. Prof. Dario Fiore – Res. Carmela Troncoso

The objective of the NEXTLEAP project is to build the fundamental interdisciplinary internet science necessary to create decentralized, secure, and rights-preserving protocols for the next generation of collective awareness platforms. The long term goal of NEXTLEAP is to have Europe take the "next leap ahead" of the rest of the world by solving the fundamental challenge of determining both how to scientifically build and help citizens and institutions adopt open-source, decentralized and privacy-preserving digital social platforms. This paradigm is in contrast to proprietary, centralized, cloud-based services and pervasive surveillance that function at the expense of rights and technological sovereignty.

TRACES

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

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2019
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.

DEDETIS

Detecting and Defending Against Threats to the Information Society

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2018
Principal Investigators: Assoc. Res. Prof. Juan Caballero – Assoc. Res. Prof. Boris Köpf

The goal of the DEDETIS project is to deliver the next generation of detection and defense techniques and tools against cyber threats. While our techniques and tools will be useful in multiple application scenarios, the emphasis of the project is on protecting the booming mobile and cloud computing environments against today's and tomorrow's threats. The work plan of the project is organized in 3 research lines that cover: 1) The fight against cybercrime, including novel system and network security approaches for detecting malicious software (malware) in mobile devices, classifying and recovering the software lineage of malware, and disrupting malicious server infrastructures hosted on cloud hosting services; 2) The detection and analysis of software vulnerabilities, including novel program analysis techniques to detect vulnerabilities with high coverage as well as algorithmic vulnerabilities, e.g., side-channel attacks on cryptographic modules and denial of service attacks through resource starvation; 3) Privacy and integrity in cloud computing , including novel cryptographic protocols based on homomorphic encryption and zero-knowledge verifiable computation to securely outsource data and computations to untrusted cloud service providers.

RISCO

Rigorous Technologies for the Analysis and Verification of Sophisticated Concurrent Software

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2018
Principal Investigators: Assoc. Res. Prof. Pierre Ganty – Assoc. Res. Prof. Alexey Gotsman

The overall goal of the project is to develop new foundations for production and rigorous formal reasoning about modern concurrent and distributed computations. Formally proving that concurrent and distributed programs behave as expected is an old problem, and many of its facets have been well understood. However, modern applications, hardware platforms, and language standards, keep imposing new and stringent requirements on the development and deployment of such programs. The specific goal of this project is to bridge the gap between the low-level details essential for the implementation of programs on modern concurrent and distributed architectures, and the high-level understanding necessary for formal verification. We will tackle the problems using a two-pronged approach, as follows: 1) We will study how the gap can be bridged in an automated way, by investigating the complexity of the verification problems for the above modern concurrent and distributed computational models, and design efficient decision procedures for reasoning about high-level abstract data types in such models, and implement them in tools; 2) We will study how the gap can be bridged in the context of human-assisted (i.e., interactive) proof development. In that setting, the challenge is to come up with proof abstractions that reduce the number and complexity of the required proof obligations, thus enabling humans to develop the correctness proofs by hand.

AxE Javascript

Auditable E-voting using Javascript

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2018
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

Computación y comunicaciones seguras en la nube para entornos hostiles

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2016-2018
Principal Investigators: Asst. 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.

RiskIoT

Sistema de monitorización proactiva en infraestructuras críticas basado en tecnologías IoT

Funding: Regional Government of Madrid
Duration: 2017-2018
Principal Investigator: Asst. Res. Prof. Alessandra Gorla

The possibility of almost instantaneously sharing data in the IoT world gives unprecedented power and, at the same time, poses great security and access control threats. It is therefore necessary to furnish new means to securely exchange data and events between the virtual and physical world. RiskIoT addresses this problem for the case of seaport environments, a critical infrastructure where a huge number of objects, companies, cameras, security sensors, persons, etc. have to safely interact and exchange information while ensuring compliance with existing legal regulations, including data provenance and privacy. The goal of RiskIoT is to provide a security middleware to make this information transmission possible, without interruptions, and abiding by the applicable laws.

Ciber4.0

Plataforma de ciberseguridad interoperable para entornos IoT en la industria 4.0

Funding: Regional Government of Madrid
Duration: 2017-2018
Principal Investigator: Assoc. Res. Prof. Juan Caballero

Internet of Things (IoT) make it possible the interconnection of many different "things" (devices, networks, systems, ...). That makes it possible a leap forward in productivity in industry. However, this brings about interoperativity and vulnerability problems that can be (and are) exploited by cybercriminals. In order to provide protection against these issues, Ciber4.0 is developing an interoperable framework that will analyze data traffic in IoT environments regardless of the protocols used or which devices are interconnected, with the aim of detecting possible security threats.

Europa Excelencia

Funding: Spanish Ministry of Economy, Industry, and Competitiveness
Duration: 2017-2019

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, by Aleksandar Nanevski, Dario Fiore and Alexey Gotsman) in the 2015 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.

POST

POST: Novel Constructions of Proof-of-Spacetime

Funding: Protocol Labs
Duration: 2018-2019
Principal Investigators: Asst. Res. Prof. Dario Fiore – Post. Res. Matteo Campanelli

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-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. Boris Köpf – Post. Res. 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, the Catholic University of Leuven, and the Technical University of Graz.

NEC

Secure Cloud Storage with Controlled Computation

Funding: NEC
Duration: 2018-2019
Principal Investigator: Asst. 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 reconciliate 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(Through an associated group at UPM.)	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
VARIES	FP7: ARTEMIS	Barco NV, HI iberia, IntegraSys, Tecnalia, 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

cont.

Project/Contract	Funding Entity	Industrial Partners
ELASTEST	H2020	Fraunhofer, Telecom Italia, Atos, Tikal Technologies, IBM Ireland, Relational
DataMantium	MINECO	Scytl
AxE Javascript	MINECO	Scytl
HC@WORKS	EIT	Atos, Thales, Engineering, CEA List
SMAPPER	EIT	Telecom Italia, Backes SRT
ANTIFRAUD	EIT	Reply SpA
MadridFlightOnChip	Madrid Regional Government	SENER, 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)	Zemsannia	Zemsania, Tecnocom, Groupalia, Solusoft, Eurona, BDigital
Contracts	NEC	NEC Laboratories Europe GmbH
Contracts	INDRA	INDRA Sistemas S.A.
Contracts (Cyber 4.0)	RedBorder	RedBorder.
Contracts (RiskIoT)	Nextel	Nextel S.A. Ingeniería y Consultoría

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. *Ramón y Cajal grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2015 and ending in 2020 (**Boris Köpf**).

4. *Estabilización Doctores I3 grant*, Spanish Ministry of Economy, Industry, and Competitiveness, awarded in 2017 and ending in 2019 (**Aleks Nanevski**).

5. *Atracción de talento Grants*, Madrid Regional Government, awarded in 2016, and ending in 2018 (**Roberto Giacobazzi**).

6. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2016 and ending in 2020 (**Elena Gutiérrez**).

7. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture, and Sports, awarded in 2017 and ending in 2021 (**Isabel García**).

8. *La Caixa Doctoral Grant*, La Caixa Foundation, awarded in 2018 and ending in 2021 (**Anaïs Querol**).

Comunidad de Madrid

EUROPEAN UNION
European Social Fund

Obra Social "la Caixa"

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

Projects to Start in 2019

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.

Comunidad de Madrid

EUROPEAN UNION

UNIVERSIDAD COMPLUTENSE MADRID

POLITÉCNICA

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, particularlyg research and demostrator satelites. 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 Ingeniería y Sistemas, which is the project coordinator.

TEZOS

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

Funding: TEZOS Foundation
Duration: 2019–2023
Principal Investigator: Assoc. Res. Prof. César Sánchez – Assoc. Res. Prof. Manuel Carro

The Tezos Foundation has developed a new partnership with IMDEA Software Institute to further maintain and advance the Tezos codebase and Tezos-related technologies. The Tezos Foundation is committed to funding world-class research that will contribute to the Tezos protocol and ecosystem. To that end, this project 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.

dissemination of results

dissemination of results


IMdea
software


uidHaskell
m Proving for All
Niki Vazou
idea
software

1. 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).

1.1. Refereed Publications

1.1.1. Journals

1. Roberto Bruni, *Roberto Giacobazzi*, Roberta Gori. Code obfuscation against abstraction refinement attacks. Formal Aspects of Computing, Vol. 30, Num. 6, pages 685–711, November 2018.

2. Dario Catalano, *Dario Fiore*, *Luca Nizzardo*. Homomorphic signatures with sublinear public keys via asymmetric programmable hash functions. Design, Codes and Cryptography, Vol. 86, Num. 10, pages 2197–2246, October 2018.

3. *Niki Vazou*, Éric Tanter, David Van Horn. Gradual Liquid Type Inference. Proc. ACM Program. Lang., Vol. 2, Num. OOPSLA, pages 1–25, ACM, October 2018.

4. Irfan Ul Haq, Sergio Chica, *Juan Caballero*, Somesh Jha. *Malware Lineage in the Wild.* Computers & Security, Vol. 78, pages 347–363, Elsevier, August 2018.

5. *Zsolt István*, David Sidler, Gustavo Alonso. *Active Pages 20 Years Later: Active Storage for the Cloud.* IEEE Internet Computing, Vol. 22, Num. 4, pages 6–14, July 2018.

6. *Anindya Banerjee*, David A. Naumann, Mohammad Nikouei. A Logical Analysis of Framing for Specifications with Pure Method Calls. ACM Trans. Program. Lang. Syst., Vol. 40, Num. 2, pages 1–90, ACM, May 2018.

7. *Nataliia Stulova*, *José F. Morales*, *Manuel V. Hermenegildo. Some Trade-offs in Reducing the Overhead of Assertion Runtime Checks via Static Analysis.* Science of Computer Programming, Vol. 155, pages 3–26, Elsevier North-Holland, April 2018. Selected and Extended papers from the 2016 International Symposium on Principles and Practice of Declarative Programming.

8. *Andrea Cerone*, *Alexey Gotsman*. *Analysing snapshot isolation.* Journal of the ACM, Vol. 65, Num. 2, pages 1–41, ACM Press, March 2018.

9. *Pedro López-García*, *Luthfi Darmawan*, Maximiliano Klemen, *Umer Liqat*, *Francisco Bueno*, *Manuel V. Hermenegildo*. Interval-based Resource Usage Verification by Translation into Horn Clauses and an Application to Energy Consumption. Theory and Practice of Logic Programming, Special Issue on Computational Logic for Verification, Vol. 18, pages 167–223, Cambridge U. Press, March 2018. arXiv:1803.04451.

10. Bishoksan Kafle, *John P. Gallagher*, *Pierre Ganty*. *Tree dimension in verification of constrained Horn clauses.* TPLP, Vol. 18, Num. 2, pages 224–251, March 2018.

11. *John P. Gallagher*, Mai Ajspur, Bishoksan Kafle. Optimised determinisation and completion of finite tree automata. Journal of Logical and Algebraic Methods in Programming, Vol. 95, pages 1–16, February 2018.

12. *Roberto Giacobazzi*, Isabella Mastroeni. Abstract Non-Interference: A Unifying Framework for Weakening Information-flow. ACM Trans. Priv. Secur., Vol. 21, Num. 2, pages 1–31, ACM, February 2018.

13. Hagit Attiya, *Alexey Gotsman*, Sandeep Hans, Noam Rinetzky. *Characterizing transactional memory consistency conditions using observational refinement.* Journal of the ACM, Vol. 65, Num. 1, pages 1–44, ACM Press, January 2018.

14. Andreas Abel, *Joakim Öhman*, Andrea Vezzosi. Decidability of conversion for type theory in type theory. Proceedings of the ACM on Programming Languages (PACMPL), Vol. 2, Num. POPL, pages 1–29, ACM, January 2018.

15. Ivan Radicek, *Gilles Barthe*, Marco Gaboardi, Deepak Garg, Florian Zuleger. Monadic refinements for relational cost analysis. PACMPL, Vol. 2, Num. POPL, pages 1–32, 2018.

16. *Gilles Barthe*, Thomas Espitau, Benjamin Grégoire, Justin Hsu, *Pierre-Yves Strub*. Proving expected sensitivity of probabilistic programs. PACMPL, Vol. 2, Num. POPL, pages 1–29, 2018.

17. Yliès Falcone, *César Sánchez*. *Introduction to the special issue on runtime verification.* Formal Methods in Systems Design, Vol. 53, Num. 1, pages 1–5, 2018.

18. Laura Bozzelli, *César Sánchez*. *Visibly Linear Temporal Logic.* Journal of Automated Reasoning, Vol. 60, Num. 2, pages 177–220, 2018.

19. *Joaquín Arias*, *Manuel Carro*, Elmer Salazar, Kyle Marple, Gopal Gupta. Constraint Answer Set Programming without Grounding. Theory and Practice of Logic Programming, Vol. 18, Num. 3-4, pages 337–354, Cambridge U. Press, 2018.

20. Dario Catalano, *Dario Fiore*. *Practical Homomorphic Message Authenticators for Arithmetic Circuits.* Journal of Cryptology, Vol. 31, Num. 1, pages 23–59, Springer, 2018.

21. Luca Aceto, Dario Della Monica, *Ignacio Fábregas*, Anna Ingólfsdóttir. *When Are Prime Formulae Characteristic?* Theoretical Computer Science, To Appear, 2018.

22. Bishoksan Kafle, *John P. Gallagher*, Graeme Gange, Peter Schachte, Harald Søndergaard, Peter J. Stuckey. An iterative approach to precondition inference using constrained Horn clauses. TPLP, Vol. 18, Num. 3-4, pages 553–570, 2018.

23. Ahmed Bouajjani, *Michael Emmi*, Constantin Enea, Jad Hamza. On reducing linearizability to state reachability. Inf. Comput., Vol. 261, Num. Part 2, pages 383–400, 2018.

1.1.2. Conferences

24. Juanru Li, Zhiqiang Lin, *Juan Caballero*, Yuanyuan Zhang, Dawu Gu. *Pinpointing Insecure Cryptographic Keys from Execution Traces.* Proceedings of the 25th ACM Conference on Computer and Communication Security, October 2018.

25. *Platon Kotzias*, Abbas Razaghpanah, Johanna Amann, Kenneth G. Paterson, Narseo Vallina-Rodríguez, *Juan Caballero*. *Coming of Age: A Longitudinal Study of TLS Deployment.* ACM Internet Measurement Conference (IMC), pages 415–428, ACM, October 2018.

26. Maximiliano Klemen, *Nataliia Stulova*, *Pedro López-García*, *José F. Morales*, *Manuel V. Hermenegildo*. *Static Performance Guarantees for Programs with Runtime Checks.* 20th Int'l. ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'18), 12 pages, ACM Press, September 2018.

27. *Dario Fiore*, Elena Pagnin. Matrioska: A Compiler for Multi-Key Homomorphic Signatures. Security and Cryptography for Networks - 11th International Conference, SCN 2018, LNCS, Vol. 11035, pages 43–62, Springer, September 2018.

28. Michel Abdalla, Dario Catalano, *Dario Fiore*, Romain Gay, Bogdan Ursu. Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings. Advances in Cryptology: Proc. of the 38th Annual Cryptology Conference (CRYPTO 2018), LNCS, Vol. 10991, pages 597–627, Springer, August 2018.

29. Zhenhao He, David Sidler, *Zsolt István*, Gustavo Alonso. *A Flexible K-Means Operator for Hybrid Databases.* Proceedings of the International Conference on Field-Programmable Logic and Applications, FPL'18, pages 368–371, August 2018.

30. *Zsolt István*, Gustavo Alonso, Ankit Singla. *Providing Multi-tenant Services with FPGAs: Case Study on a Key-Value Store.* Proceedings of the International Conference on Field-Programmable Logic and Applications, FPL'18, pages 119–124, August 2018.

31. Arianna Blasi, Alberto Goffi, Konstantin Kuznetsov, *Alessandra Gorla*, Michael D. Ernst, Mauro Pezzè, Sergio Delgado Castellanos. *Translating Code Comments to Procedure Specifications.* Proceedings of the 27th International Symposium on Software Testing and Analysis, pages 242–253, July 2018.

32. Dario Catalano, *Dario Fiore*, *Luca Nizzardo*. On the Security Notions for Homomorphic Signatures. Applied Cryptography and Network Security, ACNS 2018, LNCS, Vol. 10892, pages 183–201, Springer, June 2018.

33. Vishal Karande, Swarup Chandra, Zhiqiang Lin, *Juan Caballero*, Latifur Khan, Kevin Hamlen. BCD: Decomposing Binary Code Into Components Using Graph-Based Clustering. 13th ACM ASIA Conference on Information, Computer and Communications Security, June 2018.

34. Konstantin Kuznetsov, Vitalii Avdiienko, *Alessandra Gorla*, Andreas Zeller. *Analyzing the User Interface of Android Apps.* 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems, MOBILESoft, pages 84–87, May 2018.

35. Arianna Blasi, *Alessandra Gorla. RepliComment: Identifying Clones in Code Comments.* 2018 IEEE/ACM 26th International Conference on Program Comprehension (ICPC), pages 320–323, May 2018.

36. Paolo Calciati, Konstantin Kuznetsov, *Alessandra Gorla. What did Really Change with the new Release of the App?.* Proceedings of the 15th International Conference on Mining Software Repositories (MSR), pages 142–152, IEEE Computer Society, May 2018.

37. Chen Chen, Daniele E. Asoni, Adrian Perrig, David Barrera, George Danezis, *Carmela Troncoso. TARANET: Traffic-Analysis Resistant Anonymity at the NETwork layer.* 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2017, London, United Kindgdom, April 24-26, 2018, pages 137–152, April 2018.

38. *Nataliia Stulova*, *José F. Morales*, *Manuel V. Hermenegildo. Exploiting Term Hiding to Reduce Run-time Checking Overhead.* 20th International Symposium on Practical Aspects of Declarative Languages (PADL 2018), LNCS, Num. 10702, pages 99–115, Springer-Verlag, January 2018.

39. *Álvaro García-Pérez*, *Alexey Gotsman. Federated Byzantine quorum systems.* OPODIS'18: International Conference on Principles of Distributed Systems, LIPICS, Dagstuhl, 2018.

40. Gregory Chockler, *Alexey Gotsman. Multi-Shot Distributed Transaction Commit.* DISC'18: International Symposium on Distributed Computing, LIPICS, Vol. 121, pages 1–18, Dagstuhl, 2018.

41. *Artem Khyzha*, Hagit Attiya, *Alexey Gotsman*, Noam Rinetzky. *Safe privatization in transactional memory.* PPoPP'18: Symposium on Principles and Practice of Parallel Programming, pages 233–245, ACM Press, 2018.

42. *Álvaro García-Pérez*, *Alexey Gotsman*, *Yuri Meshman*, *Ilya Sergey. Paxos consensus, deconstructed and abstracted.* ESOP'18: European Symposium on Programming, Thessaloniki, Greece, LNCS, Vol. 10801, pages 912–939, Springer, 2018.

43. Mike Dodds, Mark Batty, *Alexey Gotsman. Compositional verification of compiler optimisations on relaxed memory.* ESOP'18: European Symposium on Programming, Thessaloniki, Greece, LNCS, Vol. 10801, pages 1027–1055, Springer, 2018.

44. *Gilles Barthe*, Xiong Fan, Joshua Gancher, Benjamin Grégoire, Charlie Jacomme, Elaine Shi. Symbolic Proofs for Lattice-Based Cryptography. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pages 538–555, ACM, 2018.

45. *Alejandro Aguirre*, *Gilles Barthe*, Justin Hsu, Alexandra Silva. Almost Sure Productivity. 45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic, LIPIcs, Vol. 107, pages 1–15, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

46. *Gilles Barthe*, Benjamin Grégoire, *Vincent Laporte*. Secure Compilation of Side-Channel Countermeasures: The Case of Cryptographic "Constant-Time". 31st IEEE Computer Security Foundations Symposium, CSF 2018, Oxford, United Kingdom, July 9-12, 2018, pages 328–343, IEEE Computer Society, 2018.

47. José Bacelar Almeida, Manuel Barbosa, *Gilles Barthe*, Hugo Pacheco, Vitor Pereira, Bernardo Portela. Enforcing Ideal-World Leakage Bounds in Real-World Secret Sharing MPC Frameworks. 31st IEEE Computer Security Foundations Symposium, CSF 2018, Oxford, United Kingdom, July 9-12, 2018, pages 132–146, IEEE Computer Society, 2018.

48. *Gilles Barthe*, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, Mehdi Tibouchi. Masking the GLP Lattice-Based Signature Scheme at Any Order. Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II, Lecture Notes in Computer Science, Vol. 10821, pages 354–384, Springer, 2018.

49. *Alejandro Aguirre*, *Gilles Barthe*, Lars Birkedal, Ales Bizjak, Marco Gaboardi, Deepak Garg. Relational Reasoning for Markov Chains in a Probabilistic Guarded Lambda Calculus. Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Lecture Notes in Computer Science, Vol. 10801, pages 214–241, Springer, 2018.

50. *Gilles Barthe*, Thomas Espitau, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, *Pierre-Yves Strub*. An Assertion-Based Program Logic for Probabilistic Programs. Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Lecture Notes in Computer Science, Vol. 10801, pages 117–144, Springer, 2018.

51. Borja Balle, *Gilles Barthe*, Marco Gaboardi. Privacy Amplification by Subsampling: Tight Analyses via Couplings and Divergences. Advances in Neural Information Processing Systems 31: Annual Conference on Neural Information Processing Systems 2018, NeurIPS 2018, 3-8 December 2018, Montréal, Canada., pages 6280–6290, 2018.

52. Apostolos Pyrgelis, *Carmela Troncoso*, Emiliano De Cristofaro. Knock Knock, Who's There? Membership Inference on Aggregate Location Data. 25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, The Internet Society, 2018.

53. Borzoo Bonakdarpour, *César Sánchez*, Gerardo Schneider. *Monitoring Hyperproperties by Combining Static Analysis and Runtime Verification.* Proc. of the 8th Int'l Symp. on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'2018). Verification. Part II, LNCS, Vol. 11245, pages 8–27, Springer, 2018.

54. *César Sánchez*, Gerardo Schneider, Martin Leucker. *Reliable Smart Contracts: State-of-the-Art, Applications, Challenges and Future Directions.* Proc. of the 8th Int'l Symp. on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'2018). Verification. Part IV, LNCS, Vol. 11247, pages 275–279, Springer, 2018.

55. Christian Colombo, Yliés Falcone, Martin Leucker, Giles Reger, *César Sánchez*, Gerardo Schneider, Volker Stolz. *COST Action IC1402 Runtime Verification Beyond Monitoring*. Proc. of the 18th Int'l Conf. on Runtime Verification (RV'18), LNCS, Vol. 11237, pages 18–26, Springer, 2018.

56. *César Sánchez. Online and Offline Stream Runtime Verification of Synchronous Systems.* Proc. of the 18th Int'l Conf. on Runtime Verification (RV'18), LNCS, Vol. 11237, pages 138–163, Springer, 2018.

57. *Felipe Gorostiaga, César Sánchez. Striver: Stream Runtime Verification for Real-Time Event-Streams.* Proc. of the 18th Int'l Conf. on Runtime Verification (RV'18), LNCS, Vol. 11237, pages 282–298, Springer, 2018.

58. Pablo Chico de Guzmán, *Felipe Gorostiaga, César Sánchez. Pipekit: A Deployment Tool with Advanced Scheduling and Inter-Service Communication for Multi-Tier Applications.* Proc. of the IEEE Int'l Conf. on Web Services (ICWS'18), pages 379–382, IEEE CS Press, 2018.

59. Pablo Chico de Guzmán, *Felipe Gorostiaga, César Sánchez. i2kit: A Deployment Tool with the Simplicity of Containers and the Security of Virtual Machines.* Proc. of the 19th Int'l Conf. on Web Information Systems Engineering (WISE 2018), Part I, LNCS, Vol. 11233, pages 81–95, Springer, 2018.

60. Raúl Pardo, *César Sánchez*, Gerardo Schneider. Timed Epistemic Knowledge Bases for Social Networks. Proc. of 22nd Int'l Symposium on Formal Methods (FM'18), LNCS, Vol. 10951, pages 185–202, Springer, 2018.

61. Martin Leucker, *César Sánchez*, Torben Scheffel, Malte Schmitz, Alexander Schramm. *TeSSLa: Runtime Verification of Non-synchronized Real-Time Streams.* Proc. of the 33rd ACM/SIGAPP Symposium on Applied Computing (SAC'17), pages 1925–1933, ACM Press, 2018. Track on Software Verification and Testing Track (SVT).

62. Maximiliano Klemen, *Nataliia Stulova, Pedro López-García, José F. Morales, Manuel V. Hermenegildo. Static Performance Guarantees for Programs with Runtime Checks.* PPDP, 12 pages, ACM Press, 2018.

63. *Umer Liqat, Zorana Banković, Pedro López-García, Manuel V. Hermenegildo. Inferring Energy Bounds via Static Program Analysis and Evolutionary Modeling of Basic Blocks.* Logic-Based Program Synthesis and Transformation - 27th International Symposium, LOPSTR 2017, Namur, Belgium, October 10-12, 2017, Revised Selected Papers, Lecture Notes in Computer Science, Vol. 10855, Springer, 2018.

64. Alejandro Z. Tomsic, *Manuel Bravo*, Marc Shapiro. Distributed Transactional Reads: The Strong, the Quick, the Fresh & the Impossible. Proceedings of the 19th International Middleware Conference, Middleware '18, pages 120–133, ACM, 2018.

65. Masayuki Abe, *Miguel Ambrona*, Miyako Ohkubo, Mehdi Tibouchi. Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings, pages 3–22, 2018.

66. *Miriam García Soto, Pavithra Prabhakar.* Averist: Algorithmic Verifier for Stability of Linear Hybrid Systems. Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (Part of CPS Week), HSCC '18, pages 259–264, ACM, 2018.

67. *Antonio Faonio*, Jesper Buus Nielsen, Mark Simkin, Daniele Venturi. Continuously Non-malleable Codes with Split-State Refresh. Applied Cryptography and Network Security - 16th International Conference, ACNS '18, pages 121–139, 2018.

68. *Pierre Ganty*, Elena Gutiérrez. *The Parikh Property for Weighted Context-Free Grammars.* 38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2018), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 122, pages 1–20, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018.

69. *Javier Esparza*, *Pierre Ganty*, Rupak Majumdar, Chana Weil-Kennedy. *Verification of Immediate Observation Population Protocols.* 29th International Conference on Concurrency Theory (CONCUR 2018), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 118, pages 1–16, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018.

70. Filippo Bonchi, *Pierre Ganty*, *Roberto Giacobazzi*, Dusko Pavlovic. Sound up-to techniques and Complete abstract domains. Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science - LICS '18, ACM Press, 2018.

71. Patrick Cousot, *Roberto Giacobazzi*, Francesco Ranzato. Program Analysis Is Harder Than Verification: A Computability Perspective. Computer Aided Verification - 30th International Conference, CAV '18, LNCS, Vol. 10982, pages 75–95, Springer, 2018.

72. Roberto Bruni, *Roberto Giacobazzi*, Roberta Gori. Code Obfuscation Against Abstract Model Checking Attacks. Verification, Model Checking, and Abstract Interpretation - 19th International Conference, VMCAI '18, LNCS, Vol. 10747, pages 94–115, Springer, 2018.

73. Cedric Baumann, Andrei Marian Dan, *Yuri Meshman*, Torsten Hoefler, Martin T. Vechev. Automatic Verification of RMA Programs via Abstraction Extrapolation. Verification, Model Checking, and Abstract Interpretation - 19th International Conference, VMCAI 2018, Los Angeles, CA, USA, January 7-9, 2018, Proceedings, pages 47–70, 2018.

1.1.3. Workshops

1. Isabel García-Contreras, *José F. Morales*, and Manuel V. Hermenegildo. *Multivariant Assertion-based Guidance in Abstract Interpretation.* Pre-proceedings of the 28th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR'18), September 2018.

2. *Pedro López-García*, Maximiliano Klemen, *Umer Liqat*, *Manuel V. Hermenegildo. A General Framework for Static Profiling of Parametric Resource Usage (extended abstract).* 19th International Workshop on Logic and Computational Complexity (LCC 2018), 4 pages, July 2018. Associated to FLOC 2018.

3. Isabel García-Contreras, *José F. Morales*, *Manuel V. Hermenegildo. Towards Incremental and Modular Context-sensitive Analysis.* Technical Communications of the 34th International Conference on Logic Programming (ICLP 2018), OpenAccess Series in Informatics (OASIcs), 2 pages, Dagstuhl Press, July 2018. (Extended Abstract).

4. Maximiliano Klemen, *Nataliia Stulova*, *Pedro López-García*, *José F. Morales*, *Manuel V. Hermenegildo. Towards Static Performance Guarantees for Programs with Run-time Checks.* Technical Communications of the 34th International Conference on Logic Programming (ICLP 2018), OpenAccess Series in Informatics (OASIcs), 2 pages, July 2018. (Extended Abstract).

5. *Serdar Erbatur*, Andrew M. Marshall, Christophe Ringeissen. *Knowledge Problems in Equational Extensions of Subterm Conver-*

gent Theories. 32nd International Workshop on Unification, July 2018.

6. Niccolò Marastoni, *Roberto Giacobazzi*, Mila Dalla Preda. A Deep Learning Approach to Program Similarity. Proceedings of the 1st International Workshop on Machine Learning and Software Engineering in Symbiosis, MASES 2018, pages 26–35, ACM, 2018.

7. *Zsolt István*, Alessandro Sorniotti, Marko Vukolić. *StreamChain: Do Blockchains Need Blocks?.* Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, SERIAL'18, pages 1–6, 2018.

1.2. Edited Volumes

1. *Alessandra Gorla*, Juan Pablo Galeotti (Eds.). Proceedings of the 11th International Workshop on Search-Based Software Testing, ICSE 2018. ACM, 2018.

2. *Gilles Barthe*, Geoff Sutcliffe, Margus Veanes (Eds.). LPAR-22. 22nd International Conference on Logic for Programming, Artificial Intelligence and Reasoning. EPiC Series in Computing, Vol. 57, EasyChair, 2018.

3. *John P. Gallagher*, Martin Sulzmann (Eds.). *Functional and Logic Programming - 14th International Symposium, FLOPS 2018, Nagoya, Japan, May 9-11, 2018, Proceedings.* Lecture Notes in Computer Science, Vol. 10818, Springer, 2018.

4. *John P. Gallagher*, Fabio Fioravanti (Eds.). *Logic-Based Program Synthesis and Transformation - 27th International Symposium, LOPSTR 2017, Namur, Belgium, October 10-12, 2017, Revised Selected Papers.* Lecture Notes in Computer Science, Vol. 10855, Springer, 2018.

5. *John P. Gallagher*, Rob van Glabbeek, Wendelin Serwe (Eds.). *Proceedings Third Workshop on Models for Formal Analysis of Real Systems and Sixth International Workshop on Verification and Program Transformation, MARS/VPT-ETAPS 2018, and Sixth International Workshop on Verification and Program Transformation Thessaloniki, Greece, 20th April 2018.* EPTCS, Vol. 268, 2018.

1.3. Articles in Books and Other Collections

1. Adrian Francalanza, Jorge A. Pérez, *César Sánchez. Runtime Verification for Decentralized and Distributed Systems.* Lectures on Runtime Verification – Introductory and Advanced Topics, LNCS, Vol. 10457, pages 169–205, Springer, 2018.

1.4. Doctoral, Master and Bachelor Theses

1. Luca Nizzardo. *Cryptographic Techniques for the Security of Cloud and Blockchain Systems.* Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). March 2018. Advisor: Dario Fiore (IMDEA Software Institute).

2. Nataliia Stulova. *Improving Run-time Checking in Dynamic Programming Languages.* Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). May 2018. Advisors: José Francisco Morales and Manuel V. Hermenegildo (IMDEA Software Institute).

3. Umer Liqat. *A Multi-Language and Multi-Platform Framework for Resource Consumption Analysis and its Application to Energy-Efficient Software Development.* Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Pedro López-García (IMDEA Software Institute).

4. Artem Khyzha. *Proving Consistency of Concurrent Data Structures and Transactional Memory Systems*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Alexey Gotsman (IMDEA Software Institute).

5. Elena Pagnin. *Be More and Be Merry: Enhancing Data and User Authentication in Collaborative Settings*. Ph.D. Thesis. Chalmers University of Technology. September 2018. Advisors: Andrei Sabelfeld (Chalmers University of Technology) and Dario Fiore (IMDEA Software Institute).

6. Miguel Ambrona. *Automated Analysis of Cryptographic Constructions*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). September 2018. Advisor: Gilles Barthe (IMDEA Software Institute).

7. Richard Rivera Guevara. *Tools for the Detection and Analysis of Potentially Unwanted Programs*. Ph.D. Thesis. Universidad Politécnica de Madrid (UPM). November 2018. Advisor: Juan Caballero (IMDEA Software Institute).

8. Felix Schroeder. *Security of Cache Replacement Policies under Side-Channel Attacks*. Master Thesis. Technical University Berlin. March 2018. Advisor: Boris Köpf (IMDEA Software Institute).

9. Felipe Gorostiaga. *Towards a Stream-Based Monitoring Language for Asynchronous Systems*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisors: César Sánchez (IMDEA Software Institute) and Lars-Ake Fredlund (UPM).

10. Gibran Alberto Gómez Montes. *Detecting and Classifying Malicious TLS Network Traffic using Machine Learning*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Juan Caballero (IMDEA Software Institute).

11. Luis Miguel Danielsson. *Decentralised Stream Runtime Verification*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisors: César Sánchez (IMDEA Software Institute) and Clara Benac Earle (UPM).

12. Paloma Pedregal Helft. *Microarchitecture Simulation for Security*. Master Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Boris Köpf (IMDEA Software Institute).

13. Mario V. García Roqué. *Sistemas criptográficos de voto electrónico basados en mix-servers y proceso de implementación*. Master Thesis. Universidad Carlos III de Madrid. September 2018. Advisors: Dario Fiore and Antonio Faonio (IMDEA Software Institute).

14. Ivan Cosmen Gancedo. *Implantación de un sistema de gestión de ventas en una compañía de venta al por menor*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Manuel Carro (IMDEA Software Institute).

15. José Luis Castañón Remy. *Web Browser-Based Interactive Crawling for Security Testing*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Avinash Sudhodanan (IMDEA Software Institute).

16. Roberto Daniel Fernández Castro. *Monitorización y Detección de Ataques en Redes Corporativas*. Bachelor Thesis. Universidad Politécnica de Madrid (UPM). July 2018. Advisor: Juan Caballero (IMDEA Software Institute).

17. Ignacio Casso San Román. *Towards Computing Distances Among Abstract Interpretations*. Bachelor Thesis. Universidad Complutense de Madrid (UCM). Septiembre 2018. Advisor: Manuel V. Hermenegildo (IMDEA Software Institute).

2 Invited Talks

2.1 Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Formal verification of side-channel resistance. International Conference on Applied Cryptography and Network Security. Leuven, Belgium. July 2018.

2. *Juan Caballero*. A Lustrum of Malware Network Communication: Evolution and Insights. Invited talk at OPTICS2 Workshop on Avionics Cybersecurity. Cologne, Germany. June 2018.

3. *Juan Caballero*. Cybersecurity 360. EIT Professional School, Munich, Germany, November 2018.

4. *Dario Fiore*. Zero-Knowledge Proofs and Applications to IoT and Blockchains. B4Things, Madrid, Spain. April 2018.

5. *Alexey Gotsman*. Reasoning about consistency choices in modern distributed systems. Workshop on Interaction and Concurrency Experiences, affiliated with International Federated Conference on Distributed Computing Techniques. Universidad Complutense de Madrid, Madrid, Spain. June 2018.

6. *Alexey Gotsman*. Tutorial: Consistency Choices in Modern Distributed Systems. PODC'18: Symposium on Principles of Distributed Computing. University of London, Egham, United Kingdom. July 2018.

7. *M.V. Hermenegildo*. 25 Years of Ciao. Invited tutorial at International Symposium on Logic-based Program Synthesis and Transformation. Frankfurt, Germany. September 2018.

8. *M.V. Hermenegildo*. Horn Clause-based Program Analysis and Verification with CiaoPP. International Workshop on Declarative Program Analysis. Amsterdam, Holland. July 2018.

2.2 Invited Seminars and Lectures by IMDEA Scientists

1. *Raúl Alborodo*. Model-based Construction of Reliable Concurrent Software. iDS Workshop Digital Infrastructure Madrid Node, Madrid, Spain. May 2018.

2. *Raúl Alborodo*. Model-based development of concurrent software. Seminar ES Unit. FBK, Trento, Italy. March 2018.

3. *Miguel Ambrona*. Criptografía: una invitación a las matemáticas. XIII Concurso matemático Miguel de Guzmán's Awards Ceremony, Rivas-Vaciamadrid, Madrid, Spain. May 2018.

4. *Miguel Ambrona*. El modelo del Grupo Genérico en Criptografía: demostraciones automáticas. Universidad Complutense de Madrid, Madrid, Spain. February 2018.

5. *Miguel Ambrona*. Matemáticas y Criptografía. ICMAT, Campus Cantoblanco UAM, Madrid, Spain. March 2018.

6. *Miguel Ambrona*. Workshop on Cryptography and Internet Security. Science Week, Universidad Complutense de Madrid, Madrid, Spain. November 2018.

7. *Alejandro Aguirre*. Almost Sure Productivity. Guest talk at Rheinisch-Westfälische Technische Hochschule Aachen (RWTH Aachen) Aachen, Germany. November 2018.

8. *Joaquín Arias*. Decoding Smart Cities Using a Rule-Based Programming Language. EIT Digital Cities Workshop, Madrid, Spain. October 2018.

9. *Joaquín Arias*. Reasoning over Stream Data Using a Rule-Based Programming Language. iDS Workshop, Madrid, Spain. May 2018.

10. *Gilles Barthe*. Formal verification of cryptographic implementations: side-channels and beyond. Alpine Verification Meeting, Wagrain, Austria. September 2018

11. *Gilles Barthe*. Security & Correctness in the IoT. Summer School, Graz, Austria. September 2018.

12. *Manuel Carro.* The Event-B Software Development Method. Tutorial at the Spanish Workshop on Programming Languages (PROLE'18). Seville, September 2018.

13. *Manuel Carro*. Horizontal Programs in Horizon 2020: The European Institute of Innovation and Technology. UPM Courses on European Project Management. March 2018.

14. *Daniel Domínguez*. Checking application behaviours against descriptions at scale. Jornadas Nacionales de Investigación en Ciberseguridad. Bilbao, Spain.

15. *Daniel Domínguez*. Checking application behaviours against descriptions at scale. Madrid Seminar on Software Research (MadSESE). Madrid, Spain. May 2018.

16. *Pierre Ganty*. Tree dimension in verification of constrained Horn clauses. Workshop on Horn Clauses for Verification and Synthesis. Oxford, UK. July 2018.

17. *Pierre Ganty*. Population protocols and predicates. International Workshop on Synthesis of Complex Parameters. Thessaloniki, Greece. April 2018.

18. *Alessandra Gorla*. Understanding the Behavior of Android apps by Means of Static and Dynamic Analyses. Summer School on Software Engineering, Free University of Bozen-Bolzano, Bolzano, Italy. July 2018.

19. *Felipe Gorostiaga*. Introduccion a Stream Runtime Verification. XVI Jornadas de Ciencias de la Computacion, Rosario, Argentina. October 2018.

20. *Alexey Gotsman*. Fast atomic broadcast over RDMA. New York University, New York, USA. October 2018.

21. *Alexey Gotsman*. Fast atomic broadcast over RDMA. Lehigh University, Bethlehem, USA. October 2018.

22. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. Yahoo Research Israel, Tel-Aviv, Israel. December 2018.

23. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. IBM Research Israel, Haifa, Israel. December 2018.

24. *Alexey Gotsman*. Atomic Transaction Commit for Modern Data Stores. Tel-Aviv University, Tel-Aviv, Israel. December 2018.

25. *Elena Gutiérrez*. The Parikh Property for Weighted Context-Free Grammars. Formal Methods and Verification Seminar, Université Libre de Bruxelles, Bruxelles, Belgium. September 2018.

26. *Joseph Izraelevitz*. Distributed Algorithms over RDMA. Microsoft Research, Cambridge, UK. July 2018.

27. *Maximiliano Klemens*. Resource-Aware Software Development. Digital Infrastructures Workshop. EIT Digital Doctoral School, Madrid Node, Madrid, Spain. May 2018.

28. *Platon Kotzias*. A Birds-Eye View of the Cyber Threat Landscape. IE Business School, Madrid, Spain. November 2018.

29. *Platon Kotzias*. Coming of Age: A Longitudinal Study of TLS Deployment. IMDEA Networks Institute, Madrid, Spain. October 2018.

30. *Platon Kotzias*. Coming of Age: A Longitudinal Study of TLS Deployment. Jornadas REDIMadrid, Madrid, Spain. October, 2018

31. *Platon Kotzias*. A Lustrum of Malware Network Communication: Evolution and Insights. Journées Nationales 2018 Pré-GDR Sécurité Informatique, Paris, France. June 2018.

32. *Boris Köpf*. Security & Correctness in the IoT. Summer School, Graz, Austria. September 2018.

33. *Aleks Nanevski*. Type and Proof Structures for Concurrent Software Verification, University of Salzburg, Salzburg, Austria. August 2018.

34. *Aleks Nanevski*. Type and Proof Structures for Concurrent Software Verification. TU Wien, Wien, Austria. August 2018.

35. *Luca Nizzardo*. Bitcoin y más allá: Cómo extender las funcionalidades de Bitcoin usando Criptografía. Codemotion Madrid 2018, Madrid, Spain. December 2018.

36. *Luca Nizzardo*. Bitcoin and Beyond (?), a Cryptographic Point of View. Invited Talk at Codemotion Blockchain and Crypto Values Conference, Milan, Italy. June 2018.

37. *Luca Nizzardo*. Bitcoin and Beyond (?). Workshop "La moneta tra Stato e Mercato, quale orizzonte per le valute virtuali". Milano-Bicocca University, Milan, Italy. April 2018.

38. *Luca Nizzardo*. Fair Exchange over Bitcoin: Zero Knowledge Contingent Payments (and more). Invited talk at Milano-Bicocca University, Department of Computer Science, , Milan, Italy. April 2018.

39. *César Sánchez*. Tutorial: "Online and Offline Stream Runtime Verification of Synchronous Systems". The 18th International Conference on Runtime Verification, Limassol, Cyprus. November 2018.

40. *Nataliia Stulova*. Verification Challenges in Dynamic Programming Languages. EPFL, Lausanne, Switzerland. August 2018.

41. *Pedro Valero*. Regular Expression Searching on Compressed Text. Seminar Series at Technical University of Munich, Munic, Germany. February 2018.

42. *Niki Vazou*. Liquid Haskell: Theorem Proving for All. Scala eXchange, London, UK. December 2018.

43. *Zsolt István*. Towards Providing Multi-tenant Services with Specialized Hardware in the Cloud. Universitatea Politehnica Bucuresti, Bucharest, Romania. September 2018.

44. *Zsolt István*. Providing Multi-tenant Services with Specialized Hardware in the Cloud. Universidad Autonoma de Madrid, Madrid, Spain. October 2018.

45. *Zsolt István*. Caribou: Building Intelligent Distributed Storage using Specialized Hardware. Technion, Haifa, Israel. November 2018.

46. *Zsolt István*. Consensus in a Box: How we Built a Replicated Key-value Store using Specialized Hardware. Universitatea Technica din Cluj-Napoca, Cluj-Napoca, Romania. November 2018.

2.3 Invited Speaker Series

During 2018, 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. *Miguel Á. Carreira-Perpiñán*. Professor, University of California at Merced, USA: Model compression as constrained optimization, with application to neural nets.

2. *Manuel Bravo*. PhD Student, University of Lisboa, Portugal: Towards a Distributed Metadata Service for Causal Consistency.

3. *Pedro Reviriego*. Associate Professor, Nebrija University, Spain: Reducing the False Positive Rate for Correlated Queries with the Adaptive Cuckoo Filter (ACF).

4. *Deepak Padmanabhan*. Lecturer, Queen's University Belfast, United Kingdom: Multi-view Data Analytics.

5. *Zsolt István*. PhD Student, ETH Zurich, Switzerland: Caribou – Intelligent Distributed Storage for the Datacenter.

6. *Fabio Palomba*. Researcher, University of Zurich, Switzerland: STATICS: Socio-Technical AnalyTICs for improving the Management of Software Evolution Tasks.

7. *Marco Guarnieri*. Post-doctoral Researcher, ETH Zurich, Switzerland: Formal foundations for access and inference control in databases.

8. *Antonio Bianchi*. PhD Student, University of California, Santa Barbara: Identifying and Mitigating Trust Violations in the Mobile Ecosystem.

9. *Samer Hassan*. Associate Research Professor, Berkman Klein Center at Harvard University & Universidad Complutense de Madrid: Decentralized Blockchain-based Organizations for Bootstrapping the Collaborative Economy.

10. *Sergio Mover*. Post-doctoral Researcher, University of Colorado Boulder, USA: Abstractions and models to design safe Event-Driven Cyber-Physical Systems.

11. *Carla Ràfols*. Post-doctoral Researcher, Universitat Pompeu Fabra, Barcelona, Spain: Efficient Zero-Knowledge Proofs or on how to use the juiciest piece of a freshly hunted SNARK.

12. *Sebastien Bardin and Richard Bonichon*. Researcher, Commissariat à l'Energie Atomique (CEA), France: Formal methods: from source-level safety to binary-level security.

13. *Jean Paul Degabriele*. Post-doctoral Researcher, TU Darmstadt, Germany: The Synergy Between Theory and Practice in Cryptography.

14. *Niki Vazou*. Post-doctoral Researcher, University of Maryland, USA: Liquid Haskell: Usable Language-Based Program Verification.

15. *Jesús López González*. PhD Student, Universidad Rey Juan Carlos & Habla Computing S.L., Spain: Optic algebras: beyond immutable data structures.

16. *Antonio Nappa*. Researcher, Minsait, Indra: Inside Spectre and Meltdown vulnerabilities.

17. *Eduardo Soria-Vázquez*. PhD Student, University of Bristol, UK: Large-Scale Secure Multi-Party Computation.

18. *Maleknaz Nayebi*. Research Professor, University of Toronto: Analytical Release Management for Mobile Apps.

19. *Itsaka Rakotonirina*. PhD Student, INRIA Nancy-Grand Est., France: The DEEPSEC Prover.

20. *Andreas Abel*. PhD Student, Saarland University, Germany: Characterizing Latency, Throughput, and Port Usage of Instructions on Intel Microarchitectures.

21. *Georg Fuchsbauer*. Research Scientist, INRIA: Subversion-resistant zero knowledge.

22. *Marco Campion*. PhD Student, University of Verona, Italy: Indexed Grammars Abstractions and Relations with other Formal Languages.

23. *Thomas Dullien*. Security Researcher, Google Project Zero: Weird Machines, Exploitability, and Provable Unexploitability.

24. *Daniel Hedin*. Senior Lecturer, Mälardalen University, Sweden: JSFlow: past, present and future.

25. *Nikita Zyuzin*. Master Student, Saarland University, Germany: Verified Checking of Finite-Precision Error Bounds using Affine Arithmetic.

26. *Nuno Machado*. Post-doctoral Researcher, INESC TEC & University of Minho, Portugal: Practical Log-based Analysis for Distributed Systems.

27. *Gerardo Schneider*. Research Professor, University of Gothenburg, Sweden: Runtime Verification of Hyperproperties for Deterministic Programs.

28. *Gibran Gómez*. Independent Researcher: Detecting and Classifying Malicious TLS Network Traffic Using Machine Learning.

29. *Steven Goldfeder*. PhD Student, Princeton University, USA: Arbitrum: Scalable Smart Contracts.

30. *Radu Iosif*. Researcher, CNRS, France: The Impact of Alternation.

31. *Jesús M. González-Barahona & Ahmed Zerouali*. Professor, Universidad Rey Juan Carlos, Spain & Bitergia, Spain: Technical lag for software deployments.

32. *Erik Derr*. Post-doctoral Researcher, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg: The Dangers of Code Reuse in (Android) Apps.

33. *Michele Orru*. PhD Student, ENS Paris: Aggregate Cash Systems: a Cryptographic Investigation of Mimblewimble.

34. *Siddharth Krishna*. PhD Student, New York University: Verifying Concurrent Search Structure Templates.

35. *Miguel Calejo & Robert Kowalski*. Logical-Contracts & Imperial College London: Logic and Smart Contracts.

2.4 Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **24** seminars were given in 2018.

3. Scientific Service and Other Activities

3.1. Conference and Program Committee Chairmanship

Gilles Barthe:

1. PC Co-Chair, 22nd International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-22).

Juan Caballero:

1. TPC Co-Chair, 2018 Annual Computer Security Applications Conference (ACSAC 2018).

John Gallagher:

1. PC Co-Chair, 14th International Symposium on Functional and Logic Programming (FLOPS 2018).
2. PC Chair of the Sixth International Workshop on Verification and Program Transformation (VPT 2018) (joint ETAPS workshop MARS/VPT@ETAPS 2018).

Alessandra Gorla:

1. PC Co-Chair, 10th International Workshop on Search-Based Software Testing (SBST 2018). ,

Niki Vazou:

1. PC co-Ccair, 3rd ACM SIGPLAN International Workshop on Type-Driven Development (TyDe 2018).

3.2. 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.
4. Steering Committee of the European Symposium on Security and Privacy (EuroS&P).

Juan Caballero:

1. Editorial Board of the ACM Transactions in Privacy and Security (ACM TOPS).
2. Steering committee of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).
3. Steering committee of Jornadas Nacionales de Investigación en Ciberseguridad (JNIC).
4. Steering Committee of the International Symposium on Engineering Secure Software and Systems (ESSoS).

Manuel Carro:

1. Area Editor, Theory and Practice of Logic Programming (Technical Notes and Rapid Publications, since July 2018).

Dario Fiore:

1. Editorial Board of IET Information Security Journal.
2. Editor Board of the International Journal of Applied Cryptography.

John Gallagher:

1. Area Editor, Theory and Practice of Logic Programming (Technical Notes and Rapid Publications, until July 2018).
2. Steering Committee. International Symposium on Functional and Logic Programming (FLOPS).

Manuel Hermenegildo:

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

Pedro López:

1. Steering Committee of the International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR)

Boris Köpf:

1. Steering committee of IEEE Computer Security Foundations Symposium (CSF).
2. Steering committee of ETAPS Conference on Principles of Security and Trust (POST).

Niki Vazou:

1. Member of Haskell Symposium Steering Committee.

3.3. Participation in Program Committees

Gilles Barthe:

1. 25th ACM Conference on Computer and Communications Security (CCS 2018).
2. 38th International Cryptology Conference (CRYPTO 2018).
3. 33rd Symposium on Logic in Computer Science (LICS 2018).
4. 45th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2018).
5. 39th IEEE Symposium on Security and Privacy (S&P 2018).

Manuel Bravo:

1. 22nd International Conference on Principles of Distributed Systems (OPODIS 2018).

Juan Caballero:

1. 13th ACM Asia Conference on Computer and Communications Security (ASIACCS 2018).
2. 39th IEEE Symposium on Security & Privacy (IEEE S&P 2018).
3. 13th Symposium on Electronic Crime Research (eCrime 2018).

Manuel Carro:

1. 34th International Conference on Logic Programming (ICLP 2018).
2. 12th International Conference on Web Services (ICWS 2018).
3. 20th International Symposium on Practical Applications of Declarative Languages (PADL 2018).
4. 18th National Workshop on Programming Languages (PROLE 2018).
5. Workshop on Logic and Practice of Programming (LPOP 2018).

Ignacio Fábregas:

1. Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics (EXPRESS/SOS 2018).

Antonio Faonio:

1. IEEE International Conference on Blockchain (Blockchain-2018).

Dario Fiore:

1. 22nd International Conference on Financial Cryptography and Data Security 2018 (FC 2018).
2. 38th International Cryptology Conference (CRYPTO 2018).
3. 25th ACM Conference on Computer and Communications Security (ACM CCS 2018).
4. 3rd International Conference on Cryptography and Information Security (BalkanCryptSec 2018).
5. III CryptoAction Symposium 2018.

John Gallagher:

1. 14th International Symposium on Functional and Logic Programming (FLOPS 2018).
2. Sixth International Workshop on Verification and Program Transformation (VPT 2018).
3. 5th Workshop on Horn Clauses for Verification and Synthesis (HCVS 2018).

Pierre Ganty:

1. 12th International Conference on Reachability Problems (RP 18).

Alessandra Gorla:

1. IEEE and ACM International Conference on Automated Software Engineering (ASE 18).

Alexey Gotsman:

1. Symposium on Principles of Distributed Computing (PODC'18).
2. International Conference on Distributed Computing Systems (ICDCS'18).
3. International Colloquium on Automata, Languages, and Programming (ICALP'18).

Manuel Hermenegildo:

1. 34th International Conference on Logic Programming (ICLP 2018).
2. International Conference on Compiler Construction (CC 2018).

Boris Köpf:

1. ACM Conference on Computer and Communication Security (CCS 2018).
2. Annual Computer Security Applications Conference (ACSAC 2018)
3. Static Analysis Symposium (SAS 2018).
4. IEEE European Symposium on Security and Privacy (EuroS&P 2018).
5. Privacy Enhancing Technologies Symposium (PETS 2018).

José Francisco Morales:

1. Doctoral Consortium (DC) on Logic Programming (ICLP-DC 2018).

Aleksandar Nanevski:

1. ACM SIGPLAN International Conference of Functional Programming (ACM ICFP 2018).
2. European Symposium on Programing (ESOP 2018).

Luca Nizzardo:

1. 11th Conference on Security and Cryptography for Networks (SCN 2018).

César Sánchez:

1. 18th International Conference on Runtime Verification (RV'18).
2. 16th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'18).
3. 16th International Conference on Software Engineering and Formal Methods (SEFM'18).
4. 3rd Workshop on Verification of Objects at RunTime EXecution (VORTEX'18).

Niki Vazou:

1. 27th European Symposium on Programming (ESOP 2018).
2. 23rd ACM SIGPLAN International Conference on Functional Programming (ICFP 2018).
3. Haskell Symposium 2018.
4. Haskell Implementors Workshop 2018.

3.4 Association and Organization Committees

Gilles Barthe:

1. International School on Foundations of Security Analysis and Design (FOSAD).
2. European Association for Theoretical Computer Science (EATCS) Summer School.
3. European Joint Conferences on Theory and Practice of Software (ETAPS) Summer School.
4. ACM Special Interest Group on Logic and Computation (SIGLOG) Summer School.
5. ACM Special Interest Group on Programming Languages (SIGPLAN) Summer School.

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.

Dario Fiore:

1. Vice-Chair and Management Committee member (representing Spain) of COST Action IC1306 "Cryptography for Secure Digital Interaction".

Manuel Hermenegildo:

1. President of the INRIA Scientific Council (Institut National de Recherche en Informatique et en Automatique, France).
2. Member of the Academia Europaea.
3. Member of the Schloss Dagstuhl Scientific Advisory Board (Germany).
4. Informatics Europe: Member of the Nomination Committee.
5. Member of the Steering Board of EIT Digital.
6. Member of the IRILL Scientific Advisory Board (French Institute for Free Software).
7. Member of the External Advisory Board of the NOVA LINCS Institute (Portugal).
8. Secretary of the International Association for Logic Programming.
9. Member of the International Federation for Computational Logic (IFCoLog) Advisory Board.
10. Member of the Technical University of Madrid Consulting Council.
11. Member of the Technical University of Madrid Gallery of Distinguished Professors.

Niki Vazou:

1. Co-organizer of Programming Languages Mentoring Worskhop (PLMW) at ICFP.
2. Member of Haskell.Org committee.

Zsolt István:

1. Co-organizer of *Birds-of-a-Feather* session at ACM Middleware'18.

César Sánchez:

1. Co-organizer of *Reliable Smart Contracts: State-of-the-art, Applications, Challenges and Future Directions* track at International Symposium On Leveraging Applications of Formal Methods, Verification and Validation.

4. Awards

4.1. Paper Awards

1. *Gilles Barthe*, Benjamin Grégoire and Vincent Laporte. Secure compilation of side-channel countermeasures: the case of cryptographic "constant-time". CSF 2018. **Distinguished paper award**.

2. Gregory Chockler and *Alexey Gotsman*. Multi-shot distributed transaction commit. International Symposium on Distributed Computing. **Best paper award**.

3. *Platon Kotzias*, Abbas Razaghpanah, Johanna Amann, Kenneth G. Paterson, Narseo Vallina-Rodríguez, *Juan Caballero*. Coming of Age: A Longitudinal Study of TLS Deployment. SIGCOMM Internet Measurement Conference. **Distinguished paper award**.

4. *Niki Vazou*, Éric Tanter, and David Van Horn. Gradual Liquid Type Inference. OOPSLA 2018. **Best Paper Award**.

4.2. Thesis Awards

1. *Umer Liquat*. Slicing probabilistic and reactive systems for model reduction. **PhD thesis Cum Laude award**.

2. *Zsolt István*. Building Distributed Storage with Specialized Hardware. **ETH Zurich Medal for Outstanding Doctoral Thesis 2018**.

3. *Nataliia Stulova*. Improving Run-time Checking in Dynamic Programming Languages. **PhD thesis Cum Laude award**.

4.3. Other Awards

1. *Silvia Sebastián*. **Community of Madrid Fellowship (Call 2018)**.

2. *Anaïs Querol*. **"La Caixa" Fellowship for Doctoral Studies at Spanish Universities or Research Centres (Call 2018).**

5. 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 2018.

1. Software Construction: Architecture and Interface Design Issues (Master level, 6 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Alessandra Gorla*.

2. Computer Security (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Juan Caballero*, *Dario Fiore*, *Alessandra Gorla*, *Marco Guarnieri*, *Boris Köpf*.

3. Formal Methods for Concurrent and Reactive System (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *César Sánchez*.

4. Abstract Interpretation (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Pierre Ganty*.

5. Rigorous Software Development (Master level, 4 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Manuel Carro*.

6. Data Structures and Algorithms (Undergraduate level, 6 ECTS). Grado en Ingeniería Informática, Universidad Politécnica de Madrid (UPM). *Manuel Carro*.

7. Security Engineering (Undergraduate level, 6 ECTS). Universidad Carlos III de Madrid (UC3M). *Juan Caballero*.

8. Seminar on Foundations of Cryptography (Master level, 2 ECTS). Master in Software and Systems (MUSS), Universidad Politécnica de Madrid (UPM). *Dario Fiore*, *Antonio Faonio*.

9. Seminar on Performance Analysis and Modelling of Software Systems (Master level, 1.5 ECTS). Universidad Politécnica de Madrid (UPM). *Zsolt István*.

10. Declarative Programming: Logic and Constraints (Undergraduate level, 3 ECTS). Grado en Ingeniería Informática, Universidad Politécnica de Madrid (UPM). *Manuel Hermenegildo*.

11. Logic and Constraint Programming. Universidad Politécnica de Madrid (UPM). *Manuel Hermenegildo*.

12. PhD training activity on Experimentation. Universidad Politécnica de Madrid (UPM). *Zsolt István*.

6. Dissemination Events

In 2018 IMDEA Software researchers have participated in multiple events related to dissemination and the promotion of science.

European Researchers' Night – IMDEA-CSI: Crime Scene Investigation (Season 2)

(9th Edition, September 28, 2018)

In September 2018, as in previous years, the IMDEA Software Institute participated in the "European Researchers' Night", coordinated by the *Fundación para el Conocimiento madrimasd*. This year's event was titled "IMDEA-CSI: Crime scene investigation (Season 2)". As in the previous edition, the IMDEA Institutes collaborated with the Spanish National Police in this event, coordinated by IMDEA Software, that showed once again how science and technology can help in solving a crime.

With undoubted police and scientific rigor, IMDEA researchers and members of the scientific Police demonstrated how research done in laboratories extends "out on the street" on many occasions, including at the scene of a crime, to assist in police work.

Radio interview

To help spread the word about the event, Manuel Carro, the Institute's Director, José Manuel Torralba, Director-General for University and Higher Art Studies, and J. Pedro Fernández, from the IMDEA Materials Institute, were interviewed in the Spanish National Radio program "Por tres razones" (For Three Reasons) on Friday, September 28th.

International Day of Women and Girls in Science

(1st Edition, February 7, 2018)

In February 2018, a round table, recorded live, was held in the IMDEA Software Institute's auditorium in order to contribute to the International Day of Women and Girls in Science. The table was moderated by journalist María José Bosch. Two researchers from IMDEA Software (Alessandra Gorla and Isabel García) and three invited professors and researchers from other institutions participated: Ernestina Menasalvas, professor at the School of Computer Science and Engineering of UPM; Asunción Santamaría, professor at the School of Telecommunication Engineering of the same University; and Elena González-Blanco, General Manager for Europe at CoverWallet and Principal Investigator of the POSTDATA ERC project.

Radio broadcast

The event was further disseminated through Gestiona Radio's program "Primera Hora", broadcasted on February 9 from 11:00 to 12:00.

News article

On February 6, 2018, the Spanish online newspaper lavanguardia.com published an article on the different activities that took place with the occasion of the International Day of Women and Girls in Science, where the round table organized by the IMDEA Software Institute was mentioned as one of such activities.

Future of Banking and AI

(June 22, 2018, El Español digital newspaper)

The director of the IMDEA Software Institute participated in a high-level meeting with several experts, namely Miquel Moya (Google), Javier Gonzalez Domínguez (Digital Innovation and Big Data, Evo Banco), Rodrigo Miranda (ISDI), Javier Iglesias (Salesforce Iberia), and Giorgio Semenzato (Finizens), to exchange their opinions on the solutions that AI can bring to banking and the challenges that this adoption can bring about.

News article

The Spanish digital newspaper, El Español, published an article after the meeting where they summarize the most important issues the speakers talked about. (https://www.elespanol.com/economia/empresas/20180621/objetivo-banca-integrada-vida-personas/316719015_0.html)

Video

The meeting was also recorded and published on the platform dailymotion. (https://www.dailymotion.com/video/x6mh04x)

Computer Science Podcasts

(September 21, 2018, 1BIT OF MEMORY)

Manuel Carro, director of the IMDEA Software Institute, contributed to the Spanish podcast "1BIT de memoria", focused on the life and achievements of great computer scientists, specifically Turing award recipients. On this occasion, the podcast focused on Leslie Lamport, widely known for his contributions to concurrent and distributed systems, verification, and for being the creator of LaTeX, one of the systems for document preparation most widely used in scientific and technical environments.

Comunidad de Madrid

EUROPEAN UNION
European Structural and Investment Fund

annual report 2018

www.software.imdea.org

imdea **software** institute

institute imdea software

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