science and technology
for developing better software

imdea **software** institute

annual report

2016

www.software.imdea.org

institute
imdea
software

foreword

foreword

Manuel Hermenegildo
Director, IMDEA Software Institute
February 11, 2017

annual report
2016

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. This is currently as relevant as ever, and software-related technology indeed has 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. 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. The Institute continues to attract to Madrid top talent worldwide, and now includes 20 faculty (one half-time), 2 associate faculty, 7 postdocs, 4 senior visitors, 30 research assistants, several interns, 16 project staff, and 7 staff members, from 17 different nationalities. Our researchers have joined the Institute after working at or obtaining their Ph.D. degrees from 32 different prestigious centers in 8 different countries, including Stanford U., Carnegie Mellon U., or Microsoft Research in the US, INRIA in France, U. of Cambridge in the UK, the Max Planck Software Institute in Germany, or ETH in Switzerland, to name just a few. In addition, more than 180 international researchers have visited and given talks at the Institute to date.

During 2016 Institute researchers have published 95 refereed publications (in some of the top venues in the field, such as POPL, ACM CCS, EUROCRYPT, IEEE S&P, USENIX Security, PODC, ISSTA CSF, CAV, ICLP, PPDP LICS, J. ACM, etc.), given 10 invited talks in international conferences and 25 invited seminars and lectures, and participated in 57 program committees and 24 boards of journals and conferences, in addition to being conference or program chairs of 14 conferences. The Institute has received 14 best paper awards or mentions in the last 5 years.

The Institute has also participated during 2016 in 33 funded research projects and contracts and received 16 fellowships. 17 of the projects are from international agencies (14 funded by the EU, 3 by the US agencies ONR and NIST), 5 are direct industrial funding, and 64% of them (21) involve collaboration with a large number of companies of all sizes, about 40% Spanish and the rest from other EU countries and the US. These include Atos, Siemens, Deimos, AbsInt, Microsoft, Fredhopper, Telefónica, Boeing, Thales, Scytl, Reply, Maxeler, XMOS, LogicBlox, France Telecom, SAP, Trusted Logic, Airbus, Alcatel, Daimler, and EADS. The Institute also commercialized in 2016 the Cadence technology with TNO and Reply.

In 2016 the Institute has also strengthened further its strategic partnership with Telefónica, Indra, Atos, and UPM, including a significant increase of the activities within the European Institute of Innovation and Technology's EIT Digital KIC. This year has seen an important expansion of the Madrid Co-Location Center, hosted and run by the Institute, and of the many other joint activities in innovation, entrepreneurship, and business development, including coaching and hosting several startups. A major achievement during 2016 has been the promotion of our node to Full Node status. The Institute has also continued its strong collaborations with Microsoft, within the Microsoft Research–IMDEA Software Joint Research Center, and with Telefónica through our Joint Research Unit. In the context of all these activities, during 2016 the Institute has hosted a good number of events centered around innovation and entrepreneurship.

Many thanks once more to all who have contributed to all these achievements, and very specially to the Madrid Regional Government and Assembly for their continuing vision and support.

table of contents

table of contents

annual report

2016

general presentation

annual report 2016

1.1. Profile

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

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

1.2. Motivation and Goals

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 European Commission data 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. 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 US 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 cyber-attacks in the European Union is in the order of billions each year. In 2013 a single data breach cost a US retail company $160 million, more than a 40% drop in its profits. Developing software technologies that can detect malicious behaviors and provide defense mechanisms against cyber-attacks 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

Modern cars and trucks contain as many as 100 million lines of computer code. This software runs on more than 30 on-board computers and controls vital functions, including the brakes, engine, cruise control, and stability systems. It is under increasing scrutiny in the wake of recent problems with major manufacturers and it is currently impossible to fully test.

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.

1.3. 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, coopera-

tion 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, and supervise the **Project Management and Technology Transfer** unit and the **Technical Support and Research Infrastructure** unit, which work closely with and support the **Research Lines** of the Institute. The current structure is depicted in Figure 1.1.

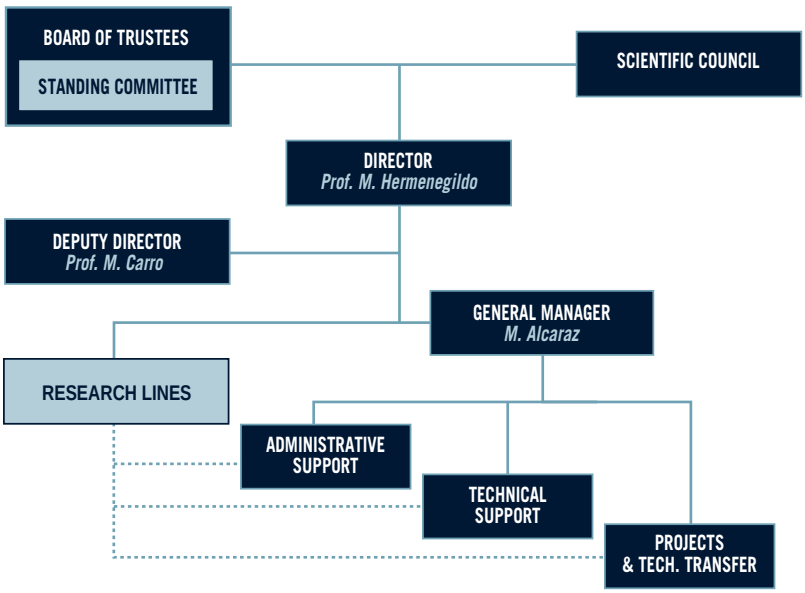


Figure 1.1. Governance and management structure of the IMDEA Software Institute.

The Board of Trustees and the Director are assisted in their functions by the **Scientific Council**, composed of high-level external scientists of international reputation with expertise in different areas of research covered by the Institute. The tasks of this scientific council 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.

1.4. Appointments to the Board of Trustees

Mr. Victor Robles Forcada, former Dean of the School of Computer Science of the Technical University of Madrid, left his position to be promoted to Vice Provost of Technology. His position in the Board of Trustees was taken by Mr. Francisco Javier Soriano Camino, current Dean of the School.

1.5. 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, Youth and Sports, Madrid Regional Government, Spain.

MADRID REGIONAL GOVERNMENT

Ilmo. Sr. D. Rafael van Grieken Salvador
Councilor for Education, Youth and Sports, Madrid Regional Government, Spain.

Ilmo. Sr. D. José Manuel Torralba Castelló
Director-General for Universities and Research, 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. Diego Córdoba Gazolaz
Consejo Superior de Investigaciones Científicas (CSIC), Spain.

Prof. Francisco Javier Soriano Camino
Dean of the School of Computer Science, 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. Luis Moniz Pereira
Universidade Nova de Lisboa, Portugal.

Prof. José Meseguer
University of Illinois at Urbana Champaign, USA.

Prof. Roberto Di Cosmo
Université Paris 7, France.

EXPERT TRUSTEES

Mr. José de la Sota Rius
Managing Director, Fundación para el Conocimiento (MadrI+D), Madrid, Spain.

Mr. Eduardo Sicilia Cavanillas
Escuela de Organización Industrial, Madrid, Spain.

INDUSTRIAL TRUSTEES

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 Telefonica Patent Office, and Estanislao Fernández González-Colaço.

Elecnor Deimos
Mr. Felipe Bertrand.

Atos
Ms. Clara Pezuela, Head of IT Market.

SECRETARY

Mr. Alejandro Blázquez Lidoy

Scientific Council

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 7, 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.

1.6. 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, part of the European Institute of Innovation and Technology, the IMDEA Software-Microsoft Joint Research Center, the IMDEA Software-Telefónica Joint Research Unit, and other joint research units with industry. 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.

industrial and institutional partnerships

annual report 2016

2.1. Industrial Partnerships

The key to innovation is in incorporating new scientific results and technologies into processes and products in a way that increases the competitiveness of industry, contributes to sustainable growth, and creates jobs. As a generator of new knowledge and technology in the high-impact area of ICT, IMDEA Software is committed to innovation and technology transfer in partnership with industry.

Collaborative Projects and Contracts. Key instruments of industrial partnership are focused collaborations with companies in the form of both *collaborative projects* funded through competitive public calls and *direct industrial contracts*. These instruments represent an excellent vehicle for performing joint research and pushing its results towards the market. Figure 2.1 lists some of the companies with which the IMDEA Software Institute has collaborated to date in such projects and contracts. The currently active projects and contracts are described further in Chapter 5.

Strategic Partnerships. The Institute has established *strategic partnerships* with the main stakeholders in the sector which facilitate longer-term collaboration across projects. In particular, the Institute has established close ties with Telefónica, Indra, Atos, and BBVA which have led to a number of strategic cooperation initiatives. An important instance of these initiatives is the joint establishment of the Spanish Associate Partner Group of EIT Digital, the ICT branch of the European Institute of Innovation and Technology, with the added participation of UPM, the Fundación General UPM, Nokia Spain, and Ferrovial, that evolved towards the status of Full Node (starting in January first, 2017) under the leadership of the Institute. The coordination of EIT Digital Madrid includes the hosting and operation of the EIT Digital Madrid Co-Location Center and many other joint activities in training (at Masters and Ph.D. level), innovation, and entrepreneurship. In addition, the Institute has established with Telefónica the *Telefónica-IMDEA Software Joint Research Unit* and with Microsoft the *Microsoft Research–IMDEA Software Joint Research Center*, and is planning the creation of more such units with other industrial partners. These activities are later described in more detail.

The participation in Spanish and EU *Technology Platforms* is another strategically important line of cooperation with industry. Such platforms include the Technology Clusters and MadridNetwork in the Madrid Region, the Internet of the Future *Es.Internet* Spanish platform, the Spanish Technology Platform for Security and Trust (eSEC, as part of the AMETIC Association), 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.

Commercialization of Technology. Another important form of technology transfer is the *commercialization of the technology* developed at the Institute. Given the controversy around software patents (and the difficulties for filing software patents in Europe), the

Institute is combining the protection of its intellectual property with other innovative exploitation models, such as those based on open-source or free software licenses, together with the licensing of such technology (e.g., the CADENCE technologies have been licensed to Communication Valley Reply), and the *creation of technology-based start-ups*. For example, five *software registrations* have been completed to date, including ActionGUI (jointly developed by IMDEA Software and ETH Zurich, for which joint work on its commercialization is also under way); GGA; EasyCrypt, ZooCrypt, and Masking (the last three developed jointly by IMDEA Software and INRIA).

Other Industrial Funding and Collaborations. Other forms of collaboration with industry include the *industrial funding of doctoral and master students* working at the Institute on industry-relevant topics (e.g., Microsoft funds research assistants working on software verification and security), *transfer of research personnel trained at the Institute to companies* (IMDEA Software-trained personnel has already been transferred to companies such as Atos, Microsoft, Google, or LogicBlox), funding by industry of *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, and a framework agreement has been signed with Microsoft for this purpose), *access to the Institute's technology and scientific results* (e.g., researchers of the Institute have presented their research results to BBVA, Telefónica I+D, Ericsson, GMV, INDRA, IBM, Canal de Isabel II, Interligare, or Lingway, among many others), access to the Institute's researchers as consultants, participation of company staff in Institute activities, etc.

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
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
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

Figure 2.1. Some companies with which the IMDEA Software Institute has collaborated through projects and contracts to date.

2.2. Cooperation with Research Institutions

As an international research organization, the Institute collaborates with many universities and other research centers worldwide. As with companies, an important way in which such cooperation happens is through focused collaborations in the framework of *collaborative projects*, funded through competitive calls or industrial contracts. At the same time, and similarly to the industrial case, the Institute has established *longer-term, strategic partnerships* with a number of research institutions, in the Madrid region and internationally, in order to allow more strategic collaborations and 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 (since November 2007).
- Universidad Complutense de Madrid (since November 2007).
- Universidad Rey Juan Carlos (since January 2008).
- Roskilde University, Denmark (since June 2008).
- Consejo Superior de Investigaciones Científicas (since November 2008).
- Swiss Federal Institute of Technology (ETH) Zurich (since November 2012).
- Microsoft Research (since December 2012, with a Joint Research Center established in 2014).

These agreements establish a framework for the development of collaborations that include the joint participation in and development of graduate programs; the joint use of resources, equipment, and infrastructure; exchange of staff; joint participation in research projects; the association of researchers and research groups with the Institute; or the joint commercialization of technology. In particular, research assistants at the IMDEA Software Institute can follow graduate studies at any of the cooperating Institutions, while funded by the IMDEA Software Institute. Furthermore, all of the seminars and talks at the Institute are open to the campus and the academic community at large.

To illustrate the scope and importance for the Institute of these agreements, we offer here some highlights. The agreement with the Universidad Politécnica de Madrid (UPM) included hosting the Institute building in its Montegancedo Science and Technology Park. In addition, the Institute has been collaborating with UPM in a graduate program for several years. This program is instrumented as a separate track on *Software Development through Rigorous Methods* in an existing Masters ("MUSS") and Ph.D. programs ("DSS / DSSC") at UPM. In them, researchers from the Institute can teach through a "Venia Docendi", i.e., a permission to teach, and be Ph.D. thesis advisors. Most research assistants at the IMDEA Software Institute obtain their Masters and Ph.D. following these programs. Under the agreement with the Consejo Superior de Investigaciones Científicas, two researchers —César Sánchez and Pedro López-García—has a dual appointment at CSIC and the Institute. 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, from the Institute's Modeling Lab. Finally, the Institute of course also collaborates with the other Institutes in the IMDEA network. As an example, the Institute has secured and coordinates the (now finished) AMAROUT-I and AMAROUT-II COFUND programs of Marie Curie fellowships, which fund 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, similar to the CRA in the US. In addition, the Institute is a member of ERCIM, the *European Research Consortium for Informatics and Mathematics* through SpaRCIM, the Spanish representative in ERCIM. Manuel Hermenegildo, IMDEA Software Institute Director, is the President of the SpaRCIM Executive Board and a member of the Informatics Europe steering board.

2.3. EIT Digital

In June 2013, IMDEA Software officially became an Associate Partner of EIT Digital (formerly known as EIT ICT Labs), as the first Spanish organization to enter its Pan-European network of 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).

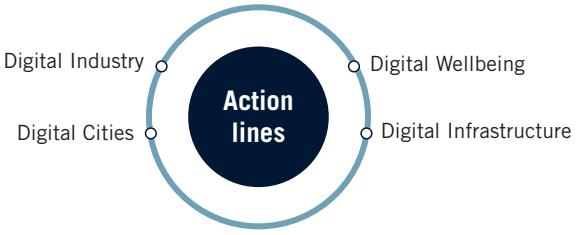
EIT Digital is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT), which includes some of the leading educational, research, and industrial actors in the ICT innovation ecosystem in Europe. Its mission is to combine the educational, research, and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

One of the key goals of IMDEA Software as the 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) – which includes some of the most prominent players in the ICT innovation arena, such as Telefónica, Indra, Atos, and the Technical University of Madrid (UPM) – towards a fully operational EIT Digital node. This goal was achieved in September 2016, with the positive vote for the candidature at the EIT Digital

General Assembly, and operation as a full node started on January 1, 2017. Becoming full node will increase the presence and leadership of Spanish partners in all activities and initiatives of EIT Digital, extending the impact on innovation. Also, the group was extended with relevant partners such as Ferrovial and two third parties: Nokia Spain and Fundación General UPM. Together with these strategic partners, the Institute is working on developing innovation-oriented projects within the framework of EIT Digital, increasing its presence in Spain through interaction with regional and national governments, and boosting and creating synergy between the entrepreneurship initiatives and mechanisms led by the members of the Spanish node and beyond.

IMDEA Software has participated in the EIT Digital Business Plan for 2016 with the following activities:

- Research and innovation activity in the field of Privacy, Security, and Trust (project SMAPPER – see Chapter 5 for more details).
- Research and innovation activity also in the field of Privacy, Security and Trust (HC@ Work – see Chapter 5 for more detail).
- Further development of the Madrid Co-Location Center (CLC), hosted in the premises of IMDEA Software. The CLC is the home for the EIT Digital activities and the meetings of the Spanish node, and has the objective of fostering innovation, technology transfer, and entrepreneurship in Spain. The CLC is equipped with ample office space and meeting facilities, workspaces for start-ups, and work and collaboration areas for the



students in the EIT Digital masters and doctoral programs. In addition to the organization and participation in relevant events devoted to innovation (e.g., matchmaking event on cybersecurity with large corporations), the CLC also hosts startups and scaleups. During 2016 three companies, participating in the EIT Digital Accelerator Program, have been coached and hosted at the CLC: Coowry, LeanXcale, and LocaliData.

- Consolidation of the Madrid Business Developers (BD) segment which is part of the EIT Digital BDA 50-strong specialist network, who help in bringing ideas to market and providing services such as coaching, access to finance, or soft landing, at a pan-European level. During 2016 the headcount was increased to four experts.
- Increase of the EIT Digital Doctoral Training Center and the Master Program in Data Analytics, in cooperation with UPM, which is part of the EIT Digital educational initiative that allows doctoral and master students to obtain not only a recognized technical education, but also entrepreneurial skills and the opportunity to work with leading business partners in European top research facilities.

2.4. Microsoft Research - IMDEA Software Joint Research Center

Joint Research Center
institute imdea software
Microsoft Research

The Microsoft Research - IMDEA Software Institute Joint Research Center (http://www.msr-imdeasw.org/) started operations in late 2013 with the objective of framing and boosting the significant research collaborations between Microsoft Research and the IMDEA Software Institute in software science and technology.

The third Microsoft Research - IMDEA Software Institute Collaborative Workshop (MICW 2016) took place at Microsoft Research in Cambridge, UK on May 3-4, 2016. This was







the third in a series of annual workshops aimed at reinforcing the collaboration between the two institutions, with researchers from both sides working together on several research topics. It was organized by Judith Bishop and Markulf Kohlweiss from Microsoft Research and by Alexey Gotsman and Manuel Hermenegildo from the IMDEA Software Institute.

The collaborative workshops bring together researchers and students to discuss their joint work on hot topics in software in order to advance the state of the art and, where possible, to bring those advances to market. The third workshop focused on three topics: Security and Cryptography, Programming Languages and Verification, Multicore and Cloud Computing.

The collaborations between IMDEA Software and Microsoft involve around 30 researchers from both sides and have resulted in more than 25 publications in top-level venues to date, including joint papers at top-ranked conferences such as ACM Symposium on Principles of Programming Languages (POPL), IEEE Symposium on Security and Privacy (S&P), and International Conference on Computer Aided Verification (CAV).

2.5. Telefónica - IMDEA Software Joint Research Unit

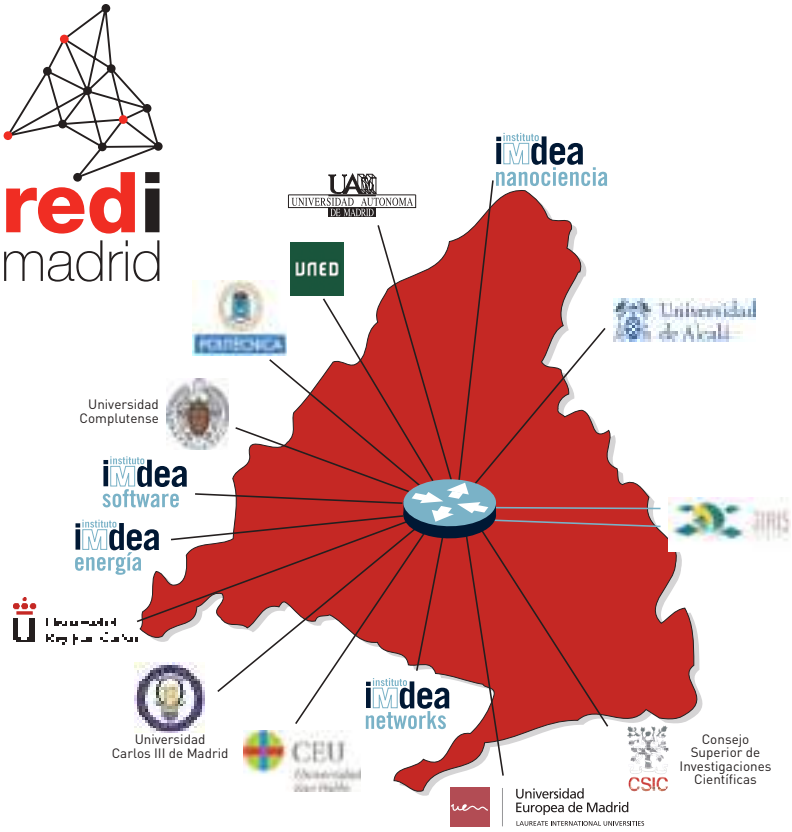
IMDEA Software and Telefónica I+D cooperate since 2012 on developing software architectures and high-level components within the framework of the FI-WARE initiative through a Joint Research Unit. This Joint Research Unit works on different topics, such as brokerage in the context of Internet of Things (IoT), and facilitating the definition and automatic deployment of cloud application components. The Joint Research Unit also organizes education activities in the area of FI-WARE technology.

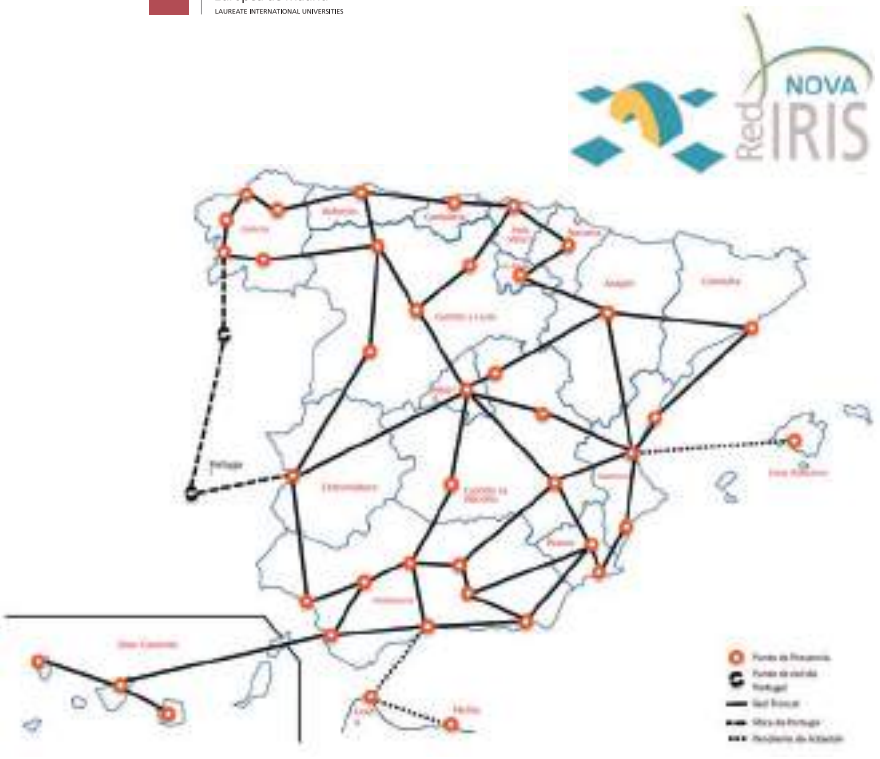
2.6. REDIMadrid

REDIMadrid is a network backbone infrastructure that connects universities and research centers within the area of Madrid. REDIMadrid is funded by the Madrid Regional Government and managed by the IMDEA Software Institute. REDIMadrid provides the connected institutions, which include the public universities in the area of Madrid and the IMDEA research institues, with a highly-reliable high-speed connection. REDIMadrid provides the communication infrastructure to these institutions to interact among themselves, to access the national network (RedIRIS), the European research network Géant and the rest of the Internet. All public universities in the area of Madrid are provided connections at 10Gb per second using a network of metropolitan fiber-optic rings, which provides a highly reliable infrastructure.

The IMDEA Software Institute also hosts and operates the new *EIT Digital node*, located at the data center of the EIT Digital Co-location Center. This node is connected 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 2016, REDIMadrid started the expansion to a modern dark fiber network with the acquisition of a link that connects the data center of Universidad Autonoma de Madrid with the REDIMadrid point of presence at CIEMAT, in Ciudad Universitaria. This link has made it possible to increase the bandwidth to fulfill the needs of the High Energy Physics research group at UAM, to provide the University with a redundant access, and to acurately assess the costs and technical needs of a full deployment that covers the whole Madrid region.


redi
madrid
imdea nanociencia
UAM
UNIVERSIDAD AUTONOMA DE MADRID
UNED
FORTHOCA
Universidad de Alcalá
Universidad Complutense
imdea software
imdea energia
IRIS
Universidad Carlos III de Madrid
CEU
imdea networks
CSIC
Consejo Superior de Investigaciones Científicas
Universidad Europea de Madrid
LAUREATE INTERNATIONAL UNIVERSITIES


Red IRIS
NOVA

research

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 and Compilers*, and *Security and Privacy*:

- Our research on *Program Analysis and Verification* advances the foundations and the tools that enable software engineers understand the key properties of the complex systems they are building. Our results range from tools that automatically establish proofs of correctness and safety, which is paramount, for example, for avionics and automotive software, to tools that explore energy consumption profiles at design time, which is fundamental for cost-effective software development in the mobile and embedded domains.

- Our research on *Languages and Compilers* 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 maintainability and reusability of software. Our results include powerful multi-paradigm programming environments as well as novel language-based techniques for building provably secure concurrent and distributed systems.

- Our research on *Security and Privacy* delivers technology that enables computation, communication, and storage in open, untrusted, and malicious enviroments, such as the Internet of Things. Our results include novel cryptographic protocols and privacy-enhancing technology, as well as cutting-edge techniques for detecting and analyzing vulnerabilities and malicious activities in software, hardware, and network traffic.

The remainder of the chapter describes in more detail the key lines of research that are currently pursued by the scientists of IMDEA Software.

3.1. "Greener" Software: Verifying and Controlling Resource Consumption

Energy consumption and the environmental impact of computing technologies is a major worldwide concern. It is a significant issue in systems ranging from energy-hungry server farms to billions of frequently charged smartphones, tablets, smart watches, sensors, and portable/implantable medical devices. As a result of the huge growth in cloud computing, Internet traffic, high-performance computing, and distributed applications, current data centers consume very large amounts of energy, not only to process and transport data, but also for cooling. Energy consumption is also highly relevant in the context of the *Internet of Things* paradigm, where very large numbers of small autonomous devices (expected to reach about 50 *billion* by the year 2020), embedded in all kind of objects, in our clothes, or stuck to our bodies, will operate and intercommunicate continuously for long periods of time, such as years. Although there have been improvements in battery and energy harvesting technology, a significant reduction in the energy demands of such devices is needed to make the full *Internet of Things* vision come true and all its potential be exploited.

In spite of the recent rapid advances in power-efficient hardware, most of the potential energy savings are wasted by software that does not exploit these hardware energy-saving features and performs poor dynamic management of tasks and resources. To face this challenge, researchers at the IMDEA Software Institute have promoted energy efficiency to a first-class goal in software design, and developed techniques and tools that facilitate the production of "greener" devices, i.e., devices that make a certifiably more efficient use of their available energy and, in general, of *resources* (e.g., execution time or memory, as well as other user-defined resources like network accesses or transactions). In particular, it is worth mentioning our novel *static profiling* techniques, which are more useful for resource-aware software development than standard resource usage analysis.

These state-of-the-art techniques and tools are implemented and integrated into the pioneering CiaoPP system, which provides a general, sound, and practical framework (based on abstract interpretation) for predicting with high accuracy the resources consumed by a given piece of software, for debugging/certifying such consumption with respect to specifications, and for generating dynamic optimization strategies. The system is adaptable to different languages, hardware, and resources because it is built around a customizable static analyzer with a versatile assertion language, in combination with

dynamic techniques for modelling. It can help programmers significantly reduce resource usage of programs, including their energy use and/or total execution time, resulting in significant improvements in battery life (e.g., in smart phones and other small devices), or reductions in electricity consumption (e.g., at data centers).

In close collaboration with industry, IMDEA's energy-aware tools are integrated into their products, and tested on concrete industrial applications. In particular, a part of this research on "greener software" has been performed within the European project ENTRA.

3.2. Concurrent Software Reliability

The importance of software reliability has dramatically increased due to the growing importance of concurrent software. Concurrent software, where different parts of a single application work at the same time, is notoriously difficult to develop, and therefore producing high-quality concurrent applications is very costly.

Concurrent software has become ubiquitous and brings novel challenges for two reasons. On one hand, modern software needs to optimize the use of new multi-core and multi-processor hardware. On the other hand, many systems are increasingly distributed (and therefore concurrent) and must respond to humans in a timely manner. This distributed nature is present both at a small scale—for example inside our mobile phones—, or at a large, Internet-sized scale, for example in social networks and planet-wide cloud systems. Modern concurrent software differs from classical approaches to concurrent programming in crucial aspects, like the structure of the synchronization —large sequential blocks of code are avoided— or the use of asynchronous programming primitives which *launch* separate tasks which need to coordinate.

Satellites have to be autonomous up to a certain degree. The programs running in their computers continuously monitor for deviations from their scheduled trajectories and take the appropriate decisions to correct them.

Testing or reasoning about modern concurrent systems requires considering a large number of interactions between the constituent components. The huge number of states to explore undermines the effectiveness of testing and leaves verification as a more appealing technique for software reliability.

New verification methods are needed to face the challenges of reliability of modern concurrent software both for specifying and assessing the correctness of concurrent programs. First, formal verification requires a description of those aspects of the behavior of a given software system that are considered crucial. New specification languages must provide this description in a way that is humanly usable and computationally tractable. Second, even though automatic verification techniques are desirable because they do not require intervention and can be applied to existing software, it is a big challenge to design automatic techniques that scale to the size of realistic programs. Alternatively, deductive techniques can handle sophisticated cases but at the cost of a higher human intervention. The challenge with deductive techniques is to increase their automation and reduce the expertise necessary to use them.

Researchers at the IMDEA Software Institute are involved in the pursuit of novel automatic and semi-automatic software verification techniques, and richer specification logics for concurrent and reactive software. These techniques are aimed at a wide range of aspects of modern concurrent software: asynchronous program verification, fine-grain and lock free algorithms, concurrent data-types, refinement of concurrent object-oriented programs, and distributed data manipulation. Apart from building the foundations to reason rigorously about these aspects of modern concurrent software, this research line also involves the development of verification tools, for example for the analysis of asynchronous concurrent software and for the deductive verification of concurrent fine-grained data-types.

3.3. Automated Software Testing and Failure Recovery

In addition to being complex, modern software poses the additional challenge that its structure evolves and often deteriorates as it grows, and it is usually unfeasible to estimate during the development phase how external factors in the execution environment will impact its behavior. This leads to faults that are difficult to anticipate. It is necessary to detect as many of these faults as possible before releasing a software artifact. However, since the complete elimination of faults is not always possible or economically feasible, it is also useful to design techniques that can mitigate the effects of previously undetected faults while the software system is running.

The predominant industrial approach to achieving software reliability is testing, in which a piece of software is exercised repeatedly trying to gain confidence that the software behaves as intended. Software testing is typically embedded in the software development life cycle to expose faults before deployment. Testing is an alternative and complementary approach to verification, which typically requires higher human expertise and is less automated. While it cannot cover all scenarios, testing is readily applicable both for small and large systems. Designing, implementing, and running tests, though, can still be very expensive. The cost of software quality assurance activities, in general, often exceeds half the overall cost of software development and maintenance. It is therefore essential to find the right balance between cost and effectiveness of quality assurance techniques.

Researchers at the IMDEA Software Institute work on designing testing techniques that are highly automated, and as a consequence cost effective. Such techniques can automatically identify test inputs that exercise the relevant features of a software artifact, can decide whether the execution of a test case matches the expected behavior, and can automatically evolve the produced test suites together with the evolution of the software artifact under development, thus limiting the costs of test case maintenance. IMDEA Software researchers also develop techniques for reducing the overhead of run-time testing, both through combination with static analysis and through better implementation techniques.

Despite the best efforts at developing effective testing and analysis techniques to detect as many faults as possible during the development phase, some faults still escape the quality control, and can ultimately affect the functionality of deployed systems. As a consequence, researchers at the IMDEA Software Institute have also been working on designing and implementing cost-effective techniques that make deployed applications more resilient to failures. Such techniques are intended to maintain a faulty application functional in the field while the developers work on more permanent fixes.

3.4. Privacy in the Digital World

The ever increasing data processing and storage capabilities enabled by technological advances open up tremendous opportunities for society, for the economy, and for individuals. However, the collection of massive amounts of electronically available information endanger values we have traditionally cherished. The inference power of modern machine learning does not only directly threaten the most basic privacy expectations of citizens, governments and corporations, but can also impact people's freedom, ultimately creating an unbalance in power relations which in turn may damage our democratic society.

Therefore, a deep understanding of the implications for privacy of the explosion of, for instance, Big Data analytics, pervasive sensors (e.g., wearables or smartphones), personalized services (e.g., personalized medicine), or de-centralization approaches (e.g., blockchain based systems) is needed in order to fully exploit the benefits of these technologies without harming the fundamental values of our society such as freedom, democracy, or equality.

In this context it is essential to provide IT system designers with means to consider privacy requirements, as well as with appropriate tools to analyze the privacy properties achieved by their designs. However, we currently lack general methodologies that allow engineers to embed privacy-preserving mechanisms in IT designs or that allow to test these mechanisms' efficacy. Instead, privacy-preserving solutions are designed and evaluated in an ad-hoc manner, hindering comparison and integration in real-world systems. Furthermore, privacy is typically in conflict with other requirements such as functionality, performance, usability, or cost. Hence, it is necessary to identify means to design systems that meet such requirements and at the same time protect the privacy of their users to a sufficient degree.

Researchers at the IMDEA Software Institute are working on the next generation of tools to put into practice the "Privacy by Design" paradigm both from the design and evaluation points of view. On the design side, the research performed at the Institute involves two aspects. First, researchers work towards the articulation of principles that allow designers and engineers to reason about privacy. Such principles ease the elicitation of privacy requirements, and guide the designer towards the best choices of system architecture and state-of-the-art privacy-preserving technologies when building IT systems that offer optimal trade-offs between privacy protection and other requirements. A second line of research involves the design of privacy-preserving cryptographic primitives that enable the outsourcing of computations without revealing data in the clear, hence preserving privacy, and the integration of such novel primitives into end-to-end secure systems that achieve concrete functionalities.

With respect to the evaluation of privacy-preserving systems, the research performed at the Institute tackles mainly two challenges. On the one hand the development of meaningful measures and metrics that allow users and analysts to agree on what it means for privacy to be "sufficiently" protected, and on the other hand the development of tools and methods that allow to systematically analyze the privacy protection offered by IT systems with respect to the developed metrics.

Recent developments at the IMDEA Software Institute in these research directions include tools to study the information leaked by cache memories, a novel method to control the amount of information leaked in shared genomic information, and a means to prove to a third party the correctness of a computation over a set of data without this party learning any information about these data.

3.5. Fighting Cybercrime and Targeted Attacks

Cyberattacks are a huge challenge to developed societies and the Internet at large. Two main threats dominate this environment: *cybercrime* and *targeted attacks*. Cybercriminals focus on economies of scale by monetizing large numbers of compromised Internet-connected hosts and their users. Users of compromised hosts can be blackmailed to pay fees for recovering their data, previously encrypted by the attacker, or incited to buy licenses for rogue software of little value. Compromised hosts can be monetized as assets for, among others, sending spam, launching denial-of-service attacks, mining virtual currencies, faking user clicks on online advertisements, or as stepping stones to hide the attacker's real location.

Targeted attacks focus on high-value targets. They have become a focus of the security industry, which has coined a new term for them, Advanced Persistent Threats (APTs), which refers to highly determined, well-funded, cyber-attackers, who persistently target an individual, group, or infrastructure. High-value targets include politicians, journalists, activists, enterprises, and critical infrastructures.

Two components are at the core of both cybercrime and targeted attacks. The first key component are malicious programs (i.e., malware) that the attacker installs on compromised Internet-connected computers. Malware enables attackers to establish a permanent presence in a compromised computer and to leverage that computer for their nefarious goals. The second key component are malicious servers, geographically distributed across the Internet, which attackers use to control the malware and to collect data exfiltrated from the compromised hosts.

Researchers at the IMDEA Software Institute are developing novel defenses against cybercrime and targeted attacks. On the malware side, during 2016 we have performed, in collaboration with Symantec Research, the first measurement of the distribution of potentially unwanted programs (PUP) such as adware and rogueware. Our analysis of 3.9 million Windows hosts showed that 54% are affected by PUP and that pay-per-install (PPI) services play a key role in their distribution. We have also developed AVClass, a massive malware labeling tool, which we have open-sourced to help researchers improve their threat intelligence analysis. On the server side, during 2016 we have developed novel active probing techniques to detect silent Web reverse proxies, which can be used by attackers to hide the location of their Web servers.

3.6. Cryptography for Next Generation Cloud Computing

Cloud computing is a fast-growing paradigm in which users lease computation resources from powerful service providers. Virtual machines, remote storage, email, web-content, databases are only some examples of services that are nowadays outsourced to the Cloud. This paradigm is very appealing to individuals and businesses due to its significant benefits: reduced IT costs, increased mobile productivity, convenient access to remote resources from multiple devices, different geographic locations, etc. The downside of cloud computing is that keeping a clear control over the data and the computations that are outsourced to the Cloud is becoming more difficult. This new working scenario exposes users to faults and attacks that are out of their control and can seriously threaten privacy and integrity of data and computations delegated to the Cloud. As an example, if the cloud provider falls under an attack, this may cause the tampering or the leakage of sensitive user data (such as credit card information or medical records) with devastating consequences.

To address these issues, researchers at the IMDEA Software Institute are working on securing the next-generation cloud infrastructure in such a way that users will be able to outsource their data and computations to untrusted providers in a fully reliable manner. The main goal of this research is to protect cloud users with respect to privacy and integrity. For privacy, cloud providers should be able to perform the operations delegated by the users without learning any unauthorized information about user data. Importantly, such strong form of privacy also prevents any attacker that would penetrate into the Cloud system from learning the content of the data therein stored. For integrity, the key idea is to enable users to verify that cloud providers have indeed operated correctly (for example, to check that the original data has not been modified without the user's authorization) without, however, spending too many resources to perform this check.

To achieve these goals, our research builds on cryptography – the science of developing methods for protecting information and communication against misbehaving parties. While initially focused on encrypted communications in the military or diplomatic domain, modern cryptography has expanded considerably and already plays a central role in the Internet. To play a similar role in the Cloud, one must design new, advanced, cryptographic mechanisms that can address privacy and integrity in this new scenario. Homomorphic encryption, verifiable computation protocols, and zero-knowledge proofs are some examples of cryptographic techniques useful in this context.

Researchers at the IMDEA Software Institute are therefore investigating novel cryptographic techniques that can achieve these advanced functionalities so that users will be able to outsource data and computations to the Cloud, and at the same time not to put their privacy and integrity at risk.

3.7. Computer-Aided Cryptographic Proofs

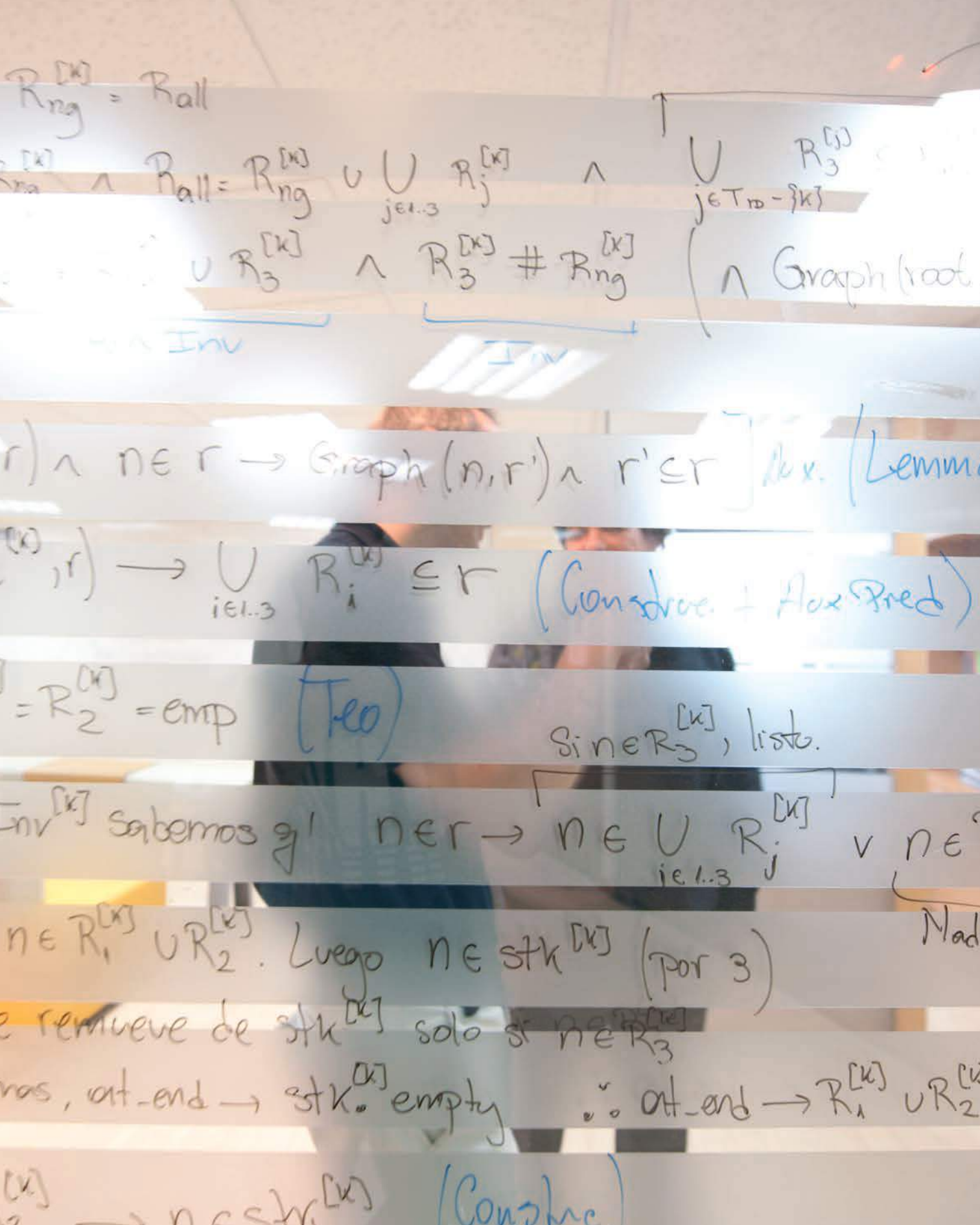
The goal of modern cryptography is to design efficient algorithms that achieve some desired functionality, and to formally prove that these algorithms guarantee a set of security requirements. Over the years, the realm of cryptography has expanded from basic primitives such as encryption, digital signatures or key exchange, to more elaborate functionalities, such as zero-knowledge protocols, or secure multi-party computation, to name a few. In many cases, these elaborate functionalities can only be built through the combination of several, elementary, cryptographic primitives. As a consequence, also proving the security of these more complex functionalities have become significantly more involved and more difficult to check. Furthermore, because cryptographic proofs are very complex, it is common practice to argue the security of cryptographic protocols at an algorithmic level, rather than at the level of implementations. This has the consequence that implementations of well-known and provably-secure cryptographic protocols are vulnerable to attacks, and regularly fail to provide their intended security guarantees.

Researchers at IMDEA Software are actively working to solve these issues, by advancing computer-aided cryptography. The main goal of this research is to develop foundations and tools that allow building and verifying the security of cryptographic protocols in an automated fashion. Additionally, it aims to verify the security guarantees at the level of implementations, thus reducing the gap between the traditional, theoretical, provable security approach and the cryptographic engineering practices.

In this domain, IMDEA researchers have explored techniques based on programming languages that allow to protect implementations of cryptographic algorithms against important classes of side-channel attacks, such as cache attacks, differential power analysis attacks and timing attacks. Notably, they developed a methodology for proving

security of implementations against timing attacks, and have shown an application of their methodology to a key component of a proof-of-concept implementation of TLS, one of the most widely used cryptographic protocols on the Internet. Their research in this area also allowed them to unveil and report an implementation bug in the S2N library by Amazon Web Services Labs.

In a related research line, IMDEA researchers have demonstrated how the methods and tools of computer-aided cryptography can be used to reason about differential privacy, a promising formal approach to data privacy, which provides a quantitative bound on the privacy cost of an algorithm that operates on sensitive information.


$R_{rng}^{[k]} = R_{all}$
$R_{all} = R_{rng}^{[k]} \cup \bigcup_{j \in 1..3} R_j^{[k]}$
$\bigcup_{j \in T_{ID} - \{k\}} R_3^{[j]}$
$\cup R_3^{[k]} \wedge R_3^{[k]} \# R_{rng}^{[k]}$
$\wedge$ Graph (root
Inv
Inv
$r) \wedge n \in r \rightarrow$ Graph $(n, r') \wedge r' \subseteq r$
Lemma
$\bigcup_{i \in 1..3} R_i^{[k]} \subseteq r$
(Construc. + Aux Pred)
$= R_2^{[k]} = emp$
(Teo)
Si $n \in R_3^{[k]}$, listo.
$Inv^{[k]}$ Sabemos q' $n \in r \rightarrow n \in \bigcup_{j \in 1..3} R_j^{[k]} \vee n \in$
$n \in R_1^{[k]} \cup R_2^{[k]}$. Luego $n \in stk^{[k]}$ (por 3)
Nad
e remueve de $stk^{[k]}$ solo si $n \in R_3^{[k]}$
ras, out_end $\rightarrow$ $stk^{[k]}$ empty $\therefore$ out_end $\rightarrow R_1^{[k]} \cup R_2^{[k]}$
$[k]$
(Construc

people

annual report 2016

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

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

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

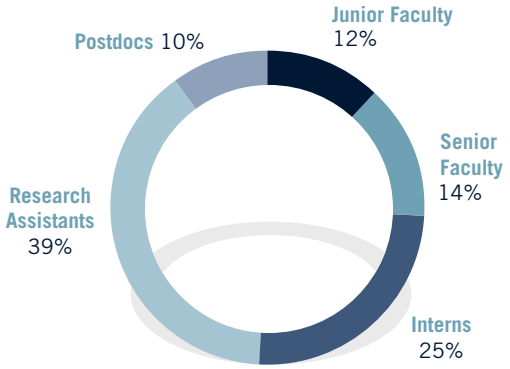


Figure 4.1. Type of position, all researchers.

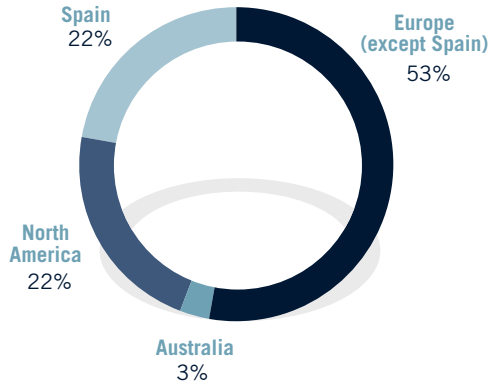


Figure 4.2. Where PhD was obtained (by continent + Spain).

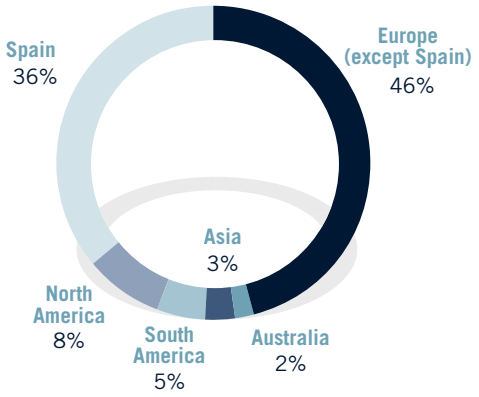


Figure 4.3. Location of previous institution, all (by continent + Spain).

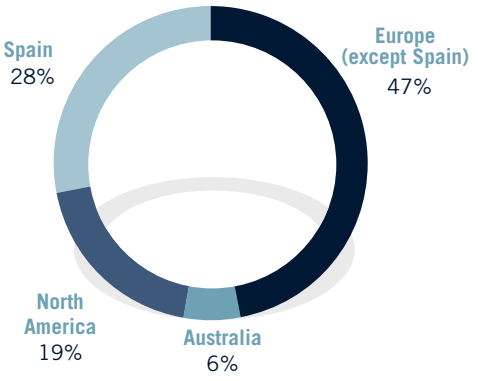


Figure 4.4. Location of previous institution of researchers at or above postdoc level (by continent + Spain).

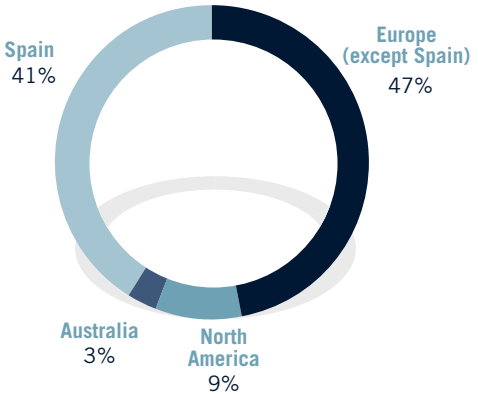


Figure 4.5. Nationality of researchers at or above postdoc level (by continent + Spain).

Status

In 2016, the scientific staff of the Institute was composed of eleven senior faculty (full or associate professors, one part-time), nine junior faculty (tenure-track or researchers), seven postdoctoral researchers, thirty research assistants (Ph.D. candidates), sixteen project staff, three system support staff, and four administrative support members (three part-time). Four senior faculty visitors and nineteen interns spent a variable length of time (from one month to a year) at the Institute collaborating with faculty members. Figure 4.1 shows the proportions of each category at the end of 2016 (where 28% were faculty members vs. 72% non-faculty). Figure 4.2 summarizes where these researchers obtained their Ph.D. (by continents plus Spain), and Figure 4.3 and Figure 4.4 show the location where the Institute researchers were working previously to joining IMDEA. Finally, Figure 4.5 presents the nationalities of researchers at or above the postdoc level.

faculty

Manuel Hermenegildo

Research Professor and Scientific Director

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. Since January 1, 2007 he is Full Professor and Scientific Director of the IMDEA Software Institute. He is also a full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining the IMDEA Software Institute he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He has also been 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 a member of the scientific boards of INRIA and Dagstuhl, among others. He has published more than 200 refereed scientific papers and monographs and has given numerous keynotes and invited talks in major conferences in these areas. He has also been coordinator and/or principal investigator of many national and international projects, area editor of several journals, and chair and PC member of a large number of conferences. He is also one of the most cited Spanish authors in Computer Science. He served as General Director for the research funding unit in Spain, as well as member of the European Union's high-level advisory group in information technology (ISTAG), and of the board of directors of the Spanish Scientific Research Council and the Center for Industrial and Technological Development, among other national and international duties.

Research Interests

His areas of interest include energy-aware computing, resource / non-functional property analysis, verification, and control; global program analysis, optimization, verification, debugging; abstract interpretation; partial evaluation; parallelism and parallelizing compilers; constraint/logic/functional programming theory and implementation; abstract machines; automatic documentation tools; execution visualization; sequential and parallel computer architecture.

Manuel Carro

Associate Research Professor and Deputy 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 Associate Research Professor and Deputy Director at the IMDEA Software Institute, and an Associate Professor at the Technical University of Madrid. He has previously been representative of UPM at the NESSI and INES technological platforms, and is now representative of UPM at SpaRCIM and deputy representative of IMDEA Software at ERCIM and Informatics Europe and CLC Manager and Scientific Coordinator of the Madrid node of EIT Digital. He has published over 70 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 being PC chair of ICLP 2016, the flagship conference in the field of Logic Programming, and 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 a European, a national, and a regional research project. He has completed the supervision of four Ph.D. theses and is actively supervising another one.

Research Interests

His interests span several topics, including the design and implementation of high-level (logic- and constraint-based) programming languages for improving the quality of software production, the analysis of service-based systems, the use of program transformation techniques for compilation on hybrid architectures, and the effective usage of formal specifications in the process of teaching programming. He has long been interested in parallel programming and parallel implementations of declarative languages, and visualization of program execution.

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 joined the IMDEA Software Institute in April 2008. Previously, he was head of the Everest team on formal methods and security at INRIA Sophia-Antipolis Méditerranée, France. He also held positions at the University of Minho, Portugal; Chalmers University, Sweden; CWI, Netherlands; University of Nijmegen, Netherlands. He has published more than 100 refereed scientific papers. He was awarded the Best Paper Awards at CRYPTO 2011 and PPoPP 2013, and was an invited speaker at numerous venues, including CSF, ESORICS, ETAPS, FAST, ITP, QEST and SAS. 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 has served as PC (co-)chair of VMCAI 2010, ESOP 2011, FAST 2011, SEFM 2011 and ESSOS 2012, and been a PC member of more than 70 conferences, including CCS, CSF, EUROCRYPT, ESORICS, FM, ICALP, LICS, and POPL. 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 interests include programming languages and program verification, software and system security, cryptography, formal methods and foundations of mathematics and computer science. Since joining IMDEA, his research has 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 chair of the Spanish Society of Software Engineering and 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, bibliometry, 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 the IMDEA Software Institute since February 2007. He is an area editor for the journal Theory and Practice of Logic Programming and has served on the program committee of approximately 60 international conferences, the executive committee of the Association for Logic Programming and the steering committee of the ACM SIGPLAN workshop on Partial Evaluation and Program Manipulation. He has published approximately 60 peer-reviewed papers which have over 2000 citations.

Research Interests

His research interests focus on program transformation and generation, constraint logic programming, rewrite systems, software verification, temporal logics, semantics-based emulation of languages and systems, analysis and verification of energy consumption and other properties of programs, and has participated in and led a number of national and European research projects on these topics. He was the scientific coordinator of the EU FET project ENTRA.

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 Spainish 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 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.

He keeps active collaborations with research groups in the USA and Europe.

Research Interests

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

Pierre Ganty

Associate Research Professor

Pierre is a researcher at the IMDEA Software Institute since the Fall 2009. He 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. Before joining the institute, Pierre did a nearly two-year postdoc at the University of California, Los Angeles (UCLA). He is the author of over 40 publications including 11 journal and 27 conference papers published in prestigious venues and accumulating more than six hundreds citations. Between 2011 and 2013 he led a Spanish national project (PARAN'10) on the verification of parameterized systems. He is currently leading a three year long Spanish national project (RISCO), started in 2016, to define rigorous techniques for the development of concurrent systems. He is supervising two Ph.D. theses and has supervised thirteen internships since he joined the Institute.

Research Interests

Pierre's research is about the algorithmic analysis of systems with infinitely many states, that is, the ability by a computer program to determine whether a given computing system (with possibly infinitely many states) comply with a given property. This is a problem of practical importance when computers are allowed to make critical decisions like how to drive cars on the roads, or medical instruments into patients. 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 has been a postdoctoral researcher at Harvard University and Microsoft Research in Cambridge, before joining IMDEA. He is a recipient of Ramon y Cajal award in 2010, and of an ERC consolidator grant in 2016.

Research Interests

His recent focus has been on developing algebraic and type-theoretic ideas that improve how we structure, on a computer, mathematical proofs about properties of programs. Structuring proofs build on the philosophy of structured programming, to identify often used but arguably harmful linguistic abstractions of the existing logics for reasoning about programs with pointers, information flow and, most recently, concurrency. Such abstractions should be replaced by better ones that provide formal mathematical proofs with more structure, and improve on the proof's conciseness, readability, development effort and maintainability.

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 Ramon y Cajal fellowship in 2016, and of an ERC starting grant in 2016.

Research Interests

Alexey's research interests are in programming models, methods and tools for developing correct concurrent and distributed software.

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 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.

Juan Caballero

Associate Research Professor

Juan Caballero joined the IMDEA Software Institute in November 2010, after receiving a Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University, USA. Prior to joining the IMDEA Software Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. Juan also holds 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. He is a recipient of the La Caixa fellowship for graduate studies.

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, cloud security, program binary analysis, and censorship resistance.

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 Incorporación fellowship awarded in 2015.

Research Interests

Dario's research interests are in Cryptography and Security. His research focuses mainly on designing provably-secure cryptographic protocols, and his recent work has particular emphasis on developing novel paradigms that provide security to Cloud computing applications. 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, 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 the IMDEA Software Institute in December 2014, she was 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.

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 Scientific Researcher position at the Spanish Council for Scientific Research (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 about 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 regional, national, and international projects.

Research Interests

His main areas of interest include automatic static energy (and resource) profiling; energy-aware software engineering; automatic analysis and verification of non-functional program properties such as resource usage (energy, execution time, user defined, etc.), non-failure and determinism; performance debugging; abstract interpretation; (automatic) granularity analysis/control for parallel and distributed computing; combined static/dynamic verification and unit-testing; tree automata; type systems; constraint and logic programming.

Pierre-Yves Strub

Researcher

Pierre-Yves Strub received his Ph.D. in Computer Science from École Polytechnique, France, in 2008. He joined the IMDEA Software Institute in 2013, after a post-doctoral position at the Microsoft-INRIA Joint Lab in Paris, France and at the LIAMA institute in Beijing, China.

Research Interests

Pierre-Yves research interests include formal proofs, proof assistants and their related type theory, certification of cryptographic algorithms and mathematical proofs, program verification via typing, and secure web programming. He is currently focused on EasyCrypt, a toolset for reasoning about relational properties of probabilistic computations with adversarial code, of which he is one of the main authors. He is also interested in the formalization of mathematics, the formal study of *Differential Power Analysis* counter-measures, and is the main author of CoqMT, an extension of the Coq proof assistant.

Michael Emmi

Researcher

Michael received his Ph.D. in Computer Science from UCLA in 2010 and joined the IMDEA Software Institute in 2013, following a postdoc fellowship at the Université Paris Diderot awarded by La Fondation Sciences Mathématiques de Paris. Prior to all that, Michael completed his undergraduate studies at Binghamton University (SUNY). He has been a teaching assistant for undergraduate courses at UCLA and Université Paris Diderot, and has held internships at Microsoft Research, NASA Ames Research Center, and IBM.

Research Interests

Michael's research enables the construction of reliable software by developing the foundations for effective programming abstractions and informative program analysis tools. Integrating technological trends with knowledge from several research communities spanning automata theory, programming languages, and distributed systems, his contributions include establishing the theoretical limits of program analysis, devising tractable approximations for intractable analysis problems, and building effective analysis tools.

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.

Jose's work to date has 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.

Research Interests

His current research interests include the design of multiparadigm languages (combining imperative, logic, functional, and object-oriented programming), assertion languages and type systems, abstract interpretation, abstract machines, compiler optimizations, and native code generation.

Benedikt Schmidt

Researcher

Benedikt Schmidt joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He received his Ph.D. degree in Computer Science from ETH Zurich, under the supervision of David Basin.

Research Interests

Benedikt is broadly interested in the areas of theorem proving, program verification, and rewriting and in their application to analyzing cryptographic systems. During his Ph.D., his work has focused on the symbolic analysis of security protocols including interactive machine-checked approaches and fully automated approaches. Since then, he has extended his focus to the computational model of attacks and is working on methods that combine the advantages of symbolic and computational models. Namely, these methods are mostly (or even fully) automated, can deal with cryptographic assumptions, cryptographic primitives, and cryptographic protocols, and provide guarantees with respect to the standard computational attacker models used in cryptography.

Alley Stoughton

Researcher

Alley Stoughton received her Ph.D. in computer science from the University of Edinburgh in 1987. Her doctoral research was on the "full abstraction" problem for programming language semantics. From 1986 until 1993, she was a research fellow and then a lecturer at the University of Sussex, where she developed an interest in implementing logic-based tools. In 1993, she joined Kansas State University as an associate professor, where she expanded her research to include functional programming. While at K-State, she designed and implemented Forlan, an open-source toolset for experimenting with formal language theory. From 2012 until 2015, she was a member of the technical staff of MIT Lincoln Laboratory, focusing on the application of formal methods and programming languages to cyber security. She joined IMDEA's Computer-Assisted Cryptography Group in 2015.

Research Interests

Alley's research applies formal methods and programming languages to cyber security. With other members of IMDEA's Computer-Assisted Cryptography Group, she is formalizing in EasyCrypt the security of NIST's SHA-3 secure hash algorithm standard. She is also using EasyCrypt to prove the security of private information retrieval cryptographic protocols. And she is researching the application of theoretical cryptography's real/ideal paradigm to the security of programs.

Carmela Troncoso

Researcher

Carmela received her Ph.D. in Engineering from the KU Leuven in 2011, where she was a student at the COSIC Group. Her thesis "Design and Analysis methods for Privacy Technologies", advised by Prof. Bart Preneel and Prof. Claudia Díaz, received the ERCIM WG Security and Trust Management Best Ph.D. Thesis Award. During her Ph.D., Carmela was a research visitor at many well-known security groups, including a three-month internship at Microsoft Research's lab in Cambridge, UK. After a year of post-doc at KULeuven she joined Gradiant, the Galician R&D Center in Advanced Telecommunications, where she became the Security and Privacy Technical Lead. At Gradiant, Carmela worked on secure and private practical solutions with local and international companies, filing one patent on vehicle-to-cloud secure communications. In October 2015 Carmela joins the IMDEA Software Institute as a Researcher.

Research Interests

Carmela's main research interests revolve around the design of privacy-preserving technologies in the digital word. Her latest research focuses on improving the level of privacy offered by decentralized systems such as those based on block chains, and on finding solutions to enable safe sharing of sensitive data, such as genetic information. She also performs research on the design of better anonymous communications systems and on the design and evaluation of location privacy-preserving mechanisms.

postdoctoral researchers

François Dupressoir

Postdoctoral researcher

François Dupressoir joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He successfully defended his Ph.D. in Computer Science at the Open University (U.K.) under the supervision of Andy Gordon, Jan Jürjens, and Bashar Nuseibeh. His Ph.D. studies were partially funded by a Microsoft Research Ph.D. scholarship, and led him to internships at the European Microsoft Innovation Center, and at Microsoft Research in Redmond and Cambridge. During those stays, he participated in the development of the VCC general-purpose verifier for C, and applied it to proving cryptographic security properties of the TPM's reference implementation.

Research Interests

François is broadly interested in program verification, theorem proving and cryptography. He is currently working on methods for formally reasoning about cryptographic security properties of real-world systems, especially focusing on obtaining strong correctness and security results on low-level implementations of schemes and protocols in presence of strong adversaries that may break abstractions, for example by observing side-channels or injecting faults in the execution of the cryptographic systems. Of particular interest is the study of how compilation can be made 'security aware', by ensuring that strong security properties are preserved by compilation, and by developing compilation techniques that prevent lower-level adversaries from exploiting their abstraction-breaking capabilities to break the security of the system.

Andrea Cerone

Postdoctoral researcher

Andrea Cerone obtained his Ph.D. in November 2012, from Trinity College Dublin. During his Ph.D. his work focused on applications of process algebras and behavioral theories to distributed systems, with a particular emphasis to wireless networks and probabilistic distributed systems. He joined the IMDEA Software Institute as a postdoctoral researcher in June 2013, his research focuses switched to the development of proof methods for verifying higher order, concurrent software, where he also started developing formal verification techniques for higher order, concurrent programs, as well as investigating the mathematical foundations of modern distributed database systems.

Research Interests

Andrea's main line of research concerns the understanding of the mathematical theory underlying modern geo-replicated and distributed databases, as well as the applications of such a theory to practical applications; these include the formal verification of concurrency control mechanisms, as well as the development of techniques for boosting the performances of geo-replicated databases. He is also interested in the understanding of behavioral theories in different concurrent models of computation. These range over a wide spectrum, including linearisability for multithreaded programs, testing preorders for distributed systems with both non-deterministic and probabilistic behavior.

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 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

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.

Giovanni Bernardi

Postdoctoral researcher

Giovanni obtained a B.Sc. and M.Sc. in computer science from Ca'Foscari, the University of Venice. During his master he spent one year studying bioinformatics at the University of Leiden. Giovanni obtained the Ph.D. from Trinity College Dublin, and after two Post-Docs, one in Dublin, and a short one at the Universidade de Lisboa, he arrived at IMDEA Software.

Research Interests

Giovanni is interested chiefly in operational and denotational semantics of programming languages for concurrent software, and in type systems for concurrency. His Ph.D. thesis unravels a series of behavioural equivalences for clients and peers within two settings, the Calculus of Communicating Systems, and higher-order session types. In subsequent work he constructed a fully-abstract semantic explanation of the standard subtyping for session types, and questioned the existing notions of duality for these types. At IMDEA Software he is working on the foundations of weak consistency levels for distributed databases, and on robustness criteria for them.

Alejandro Sánchez

Postdoctoral researcher

After obtaining his B.Sc. in Computer Science from the National University of Córdoba in Argentina, Alejandro joined the IMDEA Software Institute in 2009, first as a research intern and later as a Ph.D. Student. In 2011, he obtained his M.Sc. in Programming and Software Technology from the Complutense University of Madrid. Later, in September 2015, he obtained his Ph.D. in Computer Science from the Technical University of Madrid, where he was awarded the Outstanding Thesis award in recognition of his contributions during his Ph.D.

Research Interests

Alejandro's main research interest is the formal verification of temporal properties of safety and liveness on concurrent systems that dynamically manipulate pointer-based data structures in the heap. He is particularly interested in the formalization, development, and implementation of innovative deductive verification techniques, theories and decision procedures capable of dealing with the verification of rich properties in concurrent programs, with a special emphasis on parametrized systems.

Pablo Nogueira

Postdoctoral researcher

Pablo Nogueira joined the IMDEA Software Institute in November 2015. He holds a PhD in Computer Science from the University of Nottingham, United Kingdom, where he was funded by a studentship from the School of Computer Science and Information Technology. His thesis supervisor was Professor Roland C. Backhouse. From 2010 to 2015 he was an Assistant Professor at ETSI Informáticos, Universidad Politécnica de Madrid, where he lectured and coordinated several graduate and postgraduate courses such as Algorithms and Data Structures and Functional Programming. Before that, he held post-doctoral positions and research fellowships in Spain and the United Kingdom.

Research Interests

His research interest at large is on the theory and practice of programming and programming languages, their foundations, applications, implementations, and tools. Pablo has worked on varied topics such as generic functional programming, abstract data types and category theory, proof-directed debugging, relational algebra and unification, verification and optimisation by program transformation, operational semantics, and lambda calculi. His latest work has focused around lambda calculi and program transformation. He is also working with Associate Research Professor César Sánchez in program transformation and abstraction for fine-grained concurrent data structures.

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.

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 so as to use them in cryptographic protocols. Most of the analyses he implements are formally verified using the Coq proof assistant.

visiting and affiliate faculty

Somesh Jha
Visiting Professor

University of Wisconsin, USA

Visiting during
Sep. 2015 – Jun. 2016

Jens Grossklags
Visiting Professor

University of Pennsylvania, USA

Visiting during May. 2016 – Jul. 2016

Peter Stuckey
Visiting Professor

University of Melbourne, Australia

Visiting during
Jul. 2016–Dec. 2016

María García de la Banda
Visiting Professor

Monash University, Australia

Visiting during
Jul. 2016–Dec. 2016

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).

Julian Samborski-Forlese

Research Assistant

Research: Universidad Nacional de Rosario (UNR), Argentina.

Research: Applications of formal methods and abstract interpretation to program verification; quantum computing; functional programming languages; semantics.

Carolina Inés Dania

Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina.

Research: Software engineering, formal methods and security. In particular, working on tools and techniques for modeling, building, and validating secure and reliable software systems.

Germán Andrés Delbianco

Research Assistant

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

Research: Germán's research has focused lately on the design and implementation of new dependently-typed theories aimed at reasoning about, and proving the correctness of, higher-order programs with unstructured stateful features e.g., continuations, fork/join concurrency and coroutines, from a computational effect perspective.

Antonio Nappa

Research Assistant

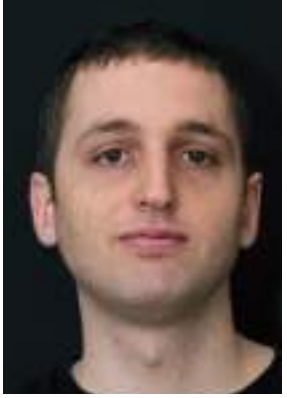
Degree: Università degli Studi di Milano, Italy.

Research: Investigating two fundamental aspects of cybercrime: vulnerability patch deployment and malicious infrastructure detection.

Umer Liqat
Research Assistant

Degree: Technical University of Madrid (UPM) and Dresden University of Technology (TUD), Germany.

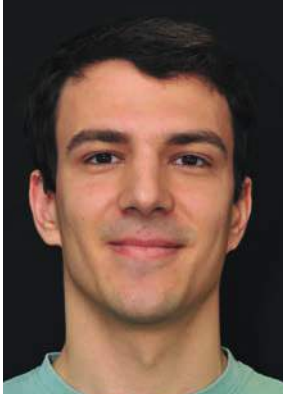
Research: Static resource analysis and verification of non-functional program properties (execution time, energy, etc.) and its applications to Energy-aware software engineering, transformation-based analysis framework for multi-language analysis and optimizations trading-off precision/performance/energy.



Goran Doychev
Research Assistant

Research: M.Sc. from Saarland University, Germany,

Research: Obtaining quantitative security guarantees for computer systems, and using them to develop economically justified defenses. Favorite application: Side-channel attacks.



Artem Khyzha
Research Assistant

Degree: 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.

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).

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 analyses.

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. He is working on the FP7 project "Whole-Systems ENergy TRAnsparency" (ENTRA).

Joaquín Arias
Research Assistant

Degree: M.SC., 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.

Damir Valput
Research Assistant

Degree: University of Zagreb, Croatia.

Research: Applications of automata theory to solving problems in formal languages, signal processing, transducers, and verification.

Miguel Ambrona
Research Assistant

Degree: 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.

Srdjan Matic
Research Assistant

Degree: Università degli Studi di Milano, Italy.

Research: Network and system security, privacy, censorship.

Irfan Ul Haq
Research Assistant

Degree: National University of Sciences and Technology (NUST), Islamabad, Pakistan.

Research: Malware unpacking, binary analysis, web security.

Raul 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.

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.

Richard Rivera
Research Assistant

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

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

Luthfi Darmawan
Research Assistant

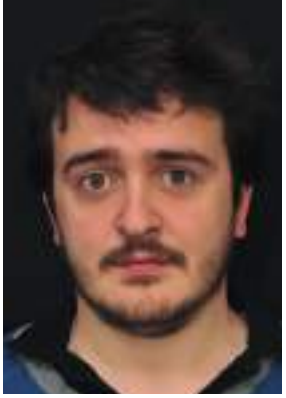
Degree: Universidad Politecnica de Madrid (UPM), Spain.

Research: Resource usage verification of computer programs.

Pablo Cañones
Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain.

Research: Information theory applied to obtaining security guaranties for cryptographic processes. I focus on the implementation of the algorithms and the hardware architectures they are run into, characterizing possible side channel attacks and obtaining security guaranties of the information leaked.



Martín Moreau
Research Assistant

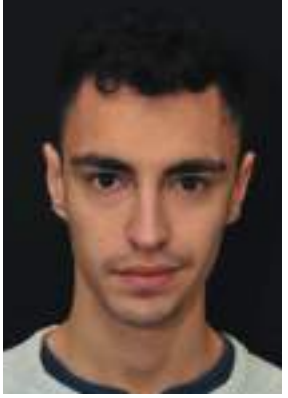
Degree: M.Sc. in Numeric Security Reliability and Performance, Université Pierre et Marie Curie (UPMC), Paris, France.

Research: Cryptography and the verification of its implementation as well as the analysis of side-channel attacks and their countermeasures.

Paolo Calciati
Research Assistant

Degree: Università della Svizzera Italiana, Lugano, Switzerland.

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



Giuseppe Guagliardo
Research Assistant

Degree: Université de Bordeaux, Bordeaux, France.

Research: Cryptography and provable security with emphasis on public key exchange protocols. Computer aided security proofs with focus on game theoretic techniques.

Pepe Vila
Research Assistant

Degree: Escuela de Ingeniería y Arquitectura de la Universidad de Zaragoza (EINA), Spain.

Research: Application security with emphasis on client-side web security, timing attacks against asynchronous systems, and side-channel countermeasures.

Alejandro Aguirre
Research Assistant

Degree: 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 Garcia
Research Assistant

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

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

Elena Gutierrez
Research Assistant

Degree: 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 Bachelor's degree in Computer Science and Mathematics at Universidad Autónoma de Madrid.

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

Bogdan Kulynych

Research Assistant

Degree: National University of Kyiv-Mohyla Academy, Ukraine.

Research: Design and implementation of privacy-preserving systems. Private and anonymous communication.

interns

Intern	Period	Nationality
Victor de Juan	Jun. 2015 – Jan. 2016	Spain
Cecile Baritel	Oct. 2015 – Jul. 2016	France
Massimo Neri	Oct. 2015 – Jan. 2016	Italy
Renzo Verastegui	Jun. 2015 – May. 2016	Romania
Marcos Sebastián	Jan. 2016 – Nov. 2016	Spain
Felix Seibert	Jan. – Apr. 2016	Germany
Daniel Henri-Mantilla	Mar. – Jul. 2016	Spain
Charlie Jacomme	Mar. – Aug. 2016	France
Alexander Schramm	Mar. – Sep. 2016	Germany
Vitor Pereira	Apr. – Jul. 2016	Portugal
Martin Zuber	Jul. 2016 – Jan. 2017	France
Anais Querol	Sep. – Dec. 2016	Spain
Silvia Sebastián	Sep. 2016 – Jan. 2017	Spain
Sergio Chica	Sep. 2016 – Jan. 2017	Spain
Sergio Delgado	Sep. 2016 – Jan. 2017	Spain
Sergio Valverde	Sep. 2016 – Jan. 2017	Spain
Chiara Redaelli	Oct. 2016 – Feb. 2017	Italy
Javier Prieto	Oct. 2016 – Jan. 2017	Spain
Borja de Regil	Oct. 2016 – Jan. 2017	Spain

project and technology

transfer staff

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.

Jesús Contreras
Business Developer, EIT Digital & Project Strategy Manager

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

Juan José Collazo
Project Manager, AMAROUT-II

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

Francisco Ibáñez
Business Developer, EIT Digital

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

Susana Eiroa
Doctoral Training Center Lead, EIT Digital

Degree: Ph.D. in Microelectronics – IMSE-CNM-CSIC, Universidad de Sevilla, Spain

Andrea Iannetta
Administrative Assistant, EIT Digital

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

Silvia Díaz-Plaza
Project Assistant, N-GREENS

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

David García
Social Media & Web Manager, EIT Digital

Degree: MA Visual Anthropology, Goldsmiths College, University of London, UK

Leandro Guillén
Technical Project Staff, Telefónica Joint Research Unit

Degree: M.Sc. in Professional Development, Universidad de Alcalá de Henares, Spain

Guillermo Jiménez
Technical Project Staff, Telefónica Joint Research Unit

Degree: B.Sc., European University Miguel de Cervantes, Valladolid, Spain

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

Carlos Rubio
Project Assistant, EIT Digital

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

Tania Rodríguez
Administrative Assistant (part-time)

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

Begoña Moreno
IMDEA Common Services (part-time)

Degree: Ph.D. in Economics and Political Sciences

Laura Bellmont
Infrastructure Manager

Degree: M.Sc. in Architecture – Technical University of Madrid (UPM), Spain.

research projects and contracts

annual report 2016

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 2016, the Institute participated in a total of 33 funded research projects and contracts, the majority of which (20, or 60%) involve collaboration with industry. Of the 33 projects, 17 are from international agencies (14 funded by the European Union and 3 by the US agencies ONR and NIST), 5 of them have direct industrial funding, and the rest are funded by national (10) and regional (1) agencies. Figure 5.1 shows the origin of project funding. In the same year, the Institute benefited from 16 fellowships. In addition, also during 2016 two grants from the European Research Council (ERC) were obtained by IMDEA Software Institute researchers.

The trend of external funding for the period 2008-2016 is shown in Figure 5.2. The amount of external funding (and the percentage of external to total funding) has risen from around 1.1 M€ (30%) in 2013 to 1.7 M€ (44%) in 2016. The level of external funding is forecast to grow to 1.8M€ in 2017, with the percentage of external funding with respect to the total Institute budget rising to 45%.

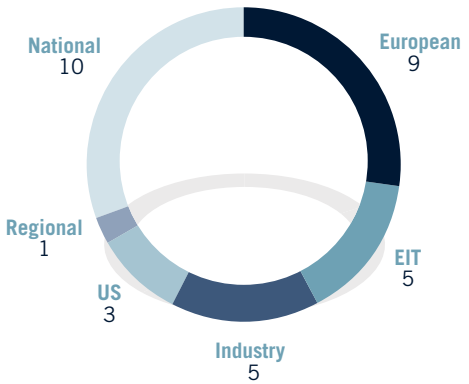


Figure 5.1. Projects by origin of funding.

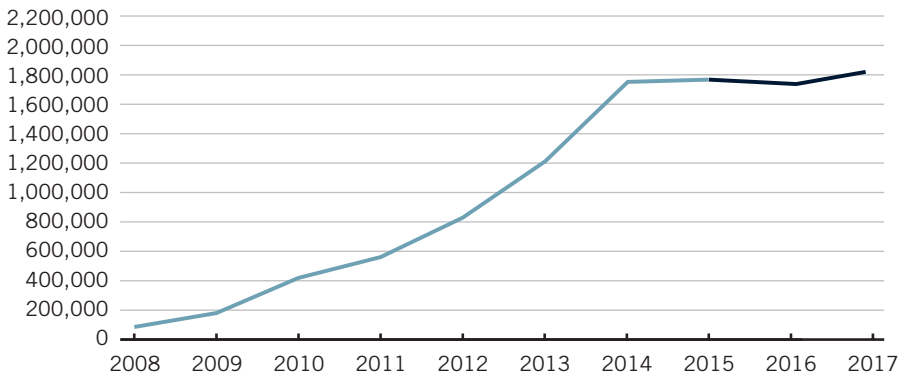


Figure 5.2. Evolution in external funding since 2008.

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 August 2018. 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.

SHA3

Verified standards: SHA3

Funding: US National Institute of Standards and Technology (NIST)
Duration: 2015-2016
Project Coordinator: Res. Prof. Gilles Barthe

The SHA3 research project is funded by NIST and runs from September 2015 until August 2016. The goal of the project is to demonstrate that the EasyCrypt tool can be used for building machine-checked, independently verifiable proofs of security for the new SHA3 standard.

The technical work will be performed in two steps. IMDEA researchers will first consider indifferentiability from a random oracle, which is among the strongest properties for hash functions and extendable-output functions, and will formalize a detailed game-based proof of indifferentiability in EasyCrypt for the sponge construction used in the SHA3 standard. Then, the IMDEA Software team will generate a C implementation from the formalization, and validate the correctness of the implementation experimentally.

EIT Digital Spain APG

APG Spain EIT Digital Coordination and Joint Activities

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2015-2017
Principal Investigator: Res. Prof. Manuel Hermenegildo

EIT Digital, as explained in section 2.3, is the Knowledge and Innovation Community (KIC) in the ICT sector of the European Institute of Innovation and Technology. The Spanish node is currently the last one to join the KIC. The Spanish node, formalized through the Associate Partner Group Spain (APG Spain), includes the following members: IMDEA Software Institute (node coordinator), Technical University of Madrid, ATOS, Indra, Telefónica, Ferrovial, Nokia Spain, and the Fundación General UPM. The coordination includes boosting the network in collaboration with members of APG 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; on the other hand to spread the activities of the APG in the national ICT sector at all levels: large companies, SMEs, entrepreneurs, students, academia and researchers. This project aims at providing support for these coordination activities in order to strengthen the position of Spain in EIT Digital.

I3H

Incubating Internet Innovation Hubs

Funding: European Union – 7th Framework Program
Duration: 2014-2016
Principal Investigator: Res. Prof. Juan José Moreno

The objective of the I3H project is to contribute to the sustainability of the Future Internet PPP (FI-PPP) by creating a European network of Internet Innovation Hubs (IIH), regional or thematic clusters that bring together web entrepreneurs, mentors, investors, students, academia, industry, and public sector innovators to speed up the transformation of FI-PPP results to services and applications addressing the needs of European citizens, companies, and society. The starting point is the network of EIT Digital hubs in Budapest, Eindhoven, Helsinki, Madrid, Paris, and Trento, where nodes of EIT Digital have their co-location centers. The seed network will grow organically with a robust life-cycle incubation stage gate process for identifying candidate hubs and guiding them through tangible milestones towards full-fledged IIH's with hands-on coaching, resources and support, including knowledge and best practice transfer.

FI-CORE

Funding: European Union – 7th Framework Program
Duration: 2014-2016
Principal Investigator: Res. Prof. Manuel Hermenegildo

The FI-Core project aims to complete the FI-PPP vision and support a truly open innovation ecosystem around FIWARE Lab, a working instance of FIWARE that is distributed across multiple data centers in Europe and is effectively operated using the suite of FIWARE Ops tools. In this project, the FI-Core consortium is delivering:

- Technology extensions, introducing new capabilities to the platform, with focus on those believed to carry substantial economic potential and future relevance. Examples include new Generic Enablers (GEs) in the areas of Robotics, Open Data, and Network Function Virtualization.

- Means for platform availability, including initiatives and processes for ensuring the effective adoption of FIWARE GE's well beyond the initial FI-PPP community. These means include the launch of operational FIWARE nodes across Europe with resources and tools to support them, as well as extensive FIWARE education and training programs for Web entrepreneurs and SMEs.

- Processes and tools for platform sustainability, ensuring outreach and dissemination of current and ongoing results from FI-Ware and Xifi projects, and their take-up by the European and global ecosystems, based on the large involvement of SMEs which will use the platform to create new value networks.

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, cyber-physical 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.

ADVENT

Architecture-Driven Verification of Systems Software

Funding: European Union – 7th Framework Program – FET Young Explorers
Duration: 2013-2016
Project Coordinator: Asst. Res. Prof. Alexey Gotsman

IMDEA Software is the main partner and coordinator of the ADVENT research project (http://advent-project.eu). The project was awarded during the year 2012 and runs from April 2013 to 2016. It is funded by the very competitive EU 7th Framework Program, Future and Emerging Technologies (FET) *Young Explorers Initiative*, and has an overall budget of 1 million Euro. In addition to IMDEA Software, the consortium includes as partners Tel Aviv University (Israel), The Max Planck Institute (Germany), and Katholieke Universiteit Leuven (Belgium).

The ADVENT project develops innovative methods and tools for cost-effective verification of real-world systems software, making it possible to guarantee an unprecedented level of reliability. ADVENT will achieve this by exploiting a trend among programmers to use informally described patterns, idioms, abstractions, and other forms of structure contained in their software, which are together called its architecture.

Building on the emerging technology of separation logic, ADVENT will formalize such software engineering concepts used by systems programmers to reason about their software informally, and will use the results to drive the design of verification techniques. This is a radically novel approach to the problem of verifying complex software: it departs from the common practice of building generic verification tools that, not being able to take advantage of programmers' knowledge and intuition, do not scale to big and complicated systems.

The architecture-driven verification techniques resulting from the project have the potential to yield a dramatic leap in the cost-benefit ratio of verification technology. This will allow verification to scale to systems of real-world size and complexity that so far have been beyond the reach of quality assurance methods guaranteeing correctness.

POLCA

Programming Large Scale Heterogeneous Infrastructures

Funding: European Union – 7th Framework Program
Duration: 2013-2016
Principal Investigator: Assoc. Res. Prof. Manuel Carro

The POLCA project explicitly addresses the programmability concerns of both embedded and high performance computing. Both domains have generated strongly focused approaches for solving their specific problems that are now confronted with the increasing need for parallelism even in Embedded Systems and the need for addressing non-functional criteria in High Performance Computing. Rather than improving both domains separately, POLCA takes a bold step forward by proposing a hybrid programming model that decisively increases programming efficiency in both areas and enables realization of multi-domain use cases.

This model thereby allows efficient parallelization and distribution of the application code across a highly heterogeneous infrastructure, not through automatic methods, but through exploitation of fundamental mathematical axioms behind the execution logic. The model is strongly oriented towards mathematical application cases of both domains, ranging from sensor evaluation, over monitoring-control-loops to complex simulation and modeling. POLCA is thereby explicitly geared towards exploitation of reconfigurable hardware to make use of their high efficiency under the right usage criteria. In principle, it even allows for exploitation of run-time reconfigurations, given an application with a suitable profile.

The project builds up on existing collaboration between experts from embedded computing and high performance computing, to combine complementary expertise from the two domains into an accessible and productive programming model of the future.

AutoCrypt

Automation in Cryptology

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2012-2016
Project Coordinator: Res. Prof. Gilles Barthe

AutoCrypt is a joint project with Stanford University, University of Pennsylvania, and SRI, funded by ONR and which runs from July 2012 until August 2016. It has an overall budget of 2 Million Euros. AutoCrypt aims to use computer technology to provide mathematical guarantees that a cryptographic algorithm is secure, and that it is adequate for a given product, process, or service.

Within the project, the IMDEA Software team use their EasyCrypt tool (http://www.easycrypt.info) to develop a systematic classification of cryptographic algorithms and to create a cryptographic atlas that will be used by researchers and companies to choose the most suitable algorithm for their needs.

StrongSoft

Sound Technologies for Reliable, Open, New Generation Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2013-2017
Principal Investigator: Res. Prof. Gilles Barthe

The goal of the StrongSoft project is to define, implement, evaluate, and disseminate disruptive technologies that are able to keep pace with the rapid evolution of software systems and address the challenges it implies. The project provides solutions for supporting the cost-effective development of a new generation of software systems that are reliable, efficient, and secure while connected to an open, untrusted world, across different application domains. The workplan is organized in a number of coordinated lines that cover security and cryptography, verification, debugging and testing, language technology, and tools. To achieve its objectives the StrongSoft consortium coordinates some of Spain's leading research groups in reliable software technologies together with a number of key foreign researchers and highly interested industrial end users.

e-TUR2020

e-TUR2020. TUrismo & Retail

Funding: Spanish Ministry of Economy and Competitiveness - CDTI
Duration: 2015-2019
Principal Investigator: Asst. 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 communication: 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.

TACLe

Timing Analysis on Code-Level

Funding: European Union, COST Action
Duration: 2015-2016
Investigator: Res. Prof. Manuel Hermenegildo

Many embedded systems are business- or safety-critical, with strict timing (and also energy) requirements. Code-level timing and energy analysis (used to analyze software running on some given hardware w.r.t. its timing properties) is an indispensable technique for ascertaining whether these requirements are met. However, recent developments in hardware, especially multi-core processors, and in software organisation render analysis increasingly more difficult, thus challenging the evolution of timing and energy analysis techniques. New principles for building "timing-composable" embedded systems are needed in order to make timing analysis tractable in the future. The goal of this Action is to gather expertise from different communities in order to develop industrial-strength code-level timing and energy analysis techniques for future-generation embedded systems.

AMAROUT II Europe

Funding: European Union, Marie Curie Action (PEOPLE-COFUND) - 7th Framework Program
Duration: 2012-2017
General Coordinator: Res. Prof. Manuel Hermenegildo

AMAROUT-II Europe is a PEOPLE-COFUND Marie Curie Action which continues the AMAROUT action sharing with it the objectives of fostering and consolidating the European Research Area by attracting top research talent to Europe and, in particular, to the region of Madrid. As in the previous AMAROUT program, "experienced" and "very experienced" researchers from any country can apply for AMAROUT II fellowships at any of the seven IMDEA Institutes participating in the program (Energy, Food, Materials, Nanoscience, Networks, Software, and Water). The program is seeking to attract, over 5 years, more than 150 experienced researchers to carry out research projects within the IMDEA network of research Institutes. The program keeps a call open permanently until month 36. Applications are evaluated by batches, according to quarterly cut-off dates. To promote the program and its calls, both nationally and abroad, best practices developed during the previous AMAROUT program are being applied. The IMDEA Software Institute is the single beneficiary of the AMAROUT-II program, the same role that was performed during the previous AMAROUT program.

As in AMAROUT, the AMAROUT-II Program is a joint initiative from the seven IMDEA research institutes. The IMDEA Software Institute was in charge of writing and submitting the proposal and is the beneficiary, acting as the administrator of the program for the other institutes.

EIT Digital CLC

Co-Location Center

The headquarters of the IMDEA Software Institute host the Madrid Co-Location Center (CLC) of EIT Digital Madrid. The CLC is the central place for organizing and implementing EIT Digital activities in Spain, and the main meeting point for the Spanish Associate Partner Group (APG), led by the IMDEA Software Institute, which includes some of the most prominent actors in the ICT innovation arena, such as Telefónica, Indra, Atos, Ferrovial, Nokia, the Technical University of Madrid (UPM), and Fundación General de la UPM (FGUPM).

EIT Digital Accelerator

The Digital Business Developers (BDs) are part of the EIT Digital BD network, and provide a group of 50 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 2016 the business acceleration activities of the Madrid APG led by the IMDEA Software Institute have been expanded to four people with a new additional expert establishing relationships with the Spanish corporate and entrepreneurship ecosystems.

EIT Digital Higher Education Schools

During 2016, the Spanish APG consolidated 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.

HC@Works

Homomorphic Cryptocomputing at WORKS

Funding: EIT Digital
Duration: 2016
Principal Investigator: Asst. Res. Prof. Dario Fiore

HC@WORKS focuses on accelerating the time to market of recently developed cryptographic techniques for protecting data privacy in real-world highly innovative software products. The main goal of HC@WORKS is to develop a suite of software tools that enable the execution of algorithms directly on encrypted data (namely, without the need to decrypt during the computation) by using *homomorphic encryption techniques*. Computing directly on encrypted information is indeed a key enabler for solving a number of privacy issues that arise when processing sensitive data on untrusted cloud computing platforms. The HC@WORKS consortium comprises six European partners from both the academic world and industry. The three applications targeted by the project are in the field of healthcare, cybersecurity and open data analytics, where privacy-preserving solutions are of crucial importance, and the innovative technologies developed in HC@WORKS will enable the creation of new privacy-enhanced versions of these products and services.

SMAPPER

Smart Mobile APP Permission Management

Funding: EIT Digital
Duration: 2016
General Coordinator: Asst. Res. Prof. Alessandra Gorla

SMAPPER is a one year-long project funded by the EIT Digital activities in 2016 in the Privacy, Security and Trust action line. The project focuses on the development of a novel technology that estimates the security and privacy risk level of Android mobile applications. SMAPPER provides three main contributions: a novel framework to analyze mobile applications at the bytecode level to report anomalous behaviors; an Android application that can inform users about suspicious apps installed on their device; an Android application that allows users to block undesired functionalities of mobile applications. The partners involved in the project are Telecom Italia (Italy), Saarland University (Germany), and Backes SRT (Germany). Alessandra Gorla and Juan Caballero from IMDEA Software were the coordinators of the project.

Microsoft Research

The strong cooperation between scientists in IMDEA Software and Microsoft Research was boosted through the opening of the Joint Research Center and the organization of the Microsoft Research and IMDEA Software Institute Cooperation Workshops (MICW). Within the Microsoft Research – IMDEA Software Joint Research Center, scientists from both sides work together on a number research topics, such as cryptography and privacy, concurrency and memory models, and programming languages and verification. The MICW has been established as an annual forum for presenting the results of the joint work. This includes a joint workshop, focused on three main topics: scalable and correct data management in the cloud, verification for cryptography and security, and secure distributed programming. MICW aims at discussing collaborative work on chosen software projects and, when possible, to bring those advances to Microsoft's businesses.

Telefónica I+D

Since 2012, IMDEA Software has cooperated with *Telefónica I+D* on research and development of components for automatic management of cloud scalability towards their integration into *Claudia*, a product developed within the European FI-WARE initiative. *Claudia* facilitates the definition and automatic deployment and management of virtual machines, storage, and connectivity resources that comprise the virtual infrastructure on which cloud applications are run. The Institute is in charge of providing advice on the software architecture and high-level design of the software components, within the FI-WARE requirements, and participates in their development and testing. The component integration is based on the OpenStack cloud architecture.

As previously mentioned, Telefónica Digital and the Institute also established during 2013 a *Joint Research Unit* (JRU) within their more global strategic partnership. This collaboration has made possible the joint participatio in FI-CORE EU Project.

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 longterm 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 and Competitiveness
Duration: 2016-2018
Project 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 and Competitiveness
Duration: 2016-2018
Project 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 and Competitiveness
Duration: 2016-2018
Project 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 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 an 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 significative 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 and Competitiveness
Duration: 2016-2018
Project 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.

Europa Excelencia

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2016-2017

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 and Alexey Gotsman) in 2015.

5.2. Some Recently Granted Projects (not started in 2016)

RACOON

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: 2017-2021
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
Project 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.

5.3. Fellowships

1. *Microsoft Research Ph.D. Scholarship funds*, active in 2013-2016 (**Boris Köpf**).

2. *Juan de la Cierva Postdoc Incorporación grant*, Spanish Ministry of Science and Innovation, awarded in 2015 and ending in 2017 (**Dario Fiore**).

3. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2016 and ending in 2021 (**Alexey Gotsman**).

4. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2015 and ending in 2020 (**Boris Köpf**).

5. *Marie Curie AMAROUT II Incoming Fellowships (7)*, European Union – Framework Program, awarded in 2012 and active in 2016 (**Dario Fiore**, **Michael Emmi**, **François Dupressoir**, **Benedikt Schmidt**, **Pierre-Yves Strub, Giovanni Bernardi** and **Alessandra Gorla**).

6. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, active in 2016 (**Miriam García**).

7. *FPI short stays support*, Spanish Ministry of Science and Innovation, in 2016 (**Miriam García**).

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

9. *Predoctoral Grants*, Madrid Regional Government, awarded in 2016, and ending in 2018 (**Isabel García**).

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

dissemination of results

annual report 2016

publications

6.1. Publications

6.1.1. Refereed Publications

Journals

1. Reza Shokri, George Theodorakopoulos, Carmela Troncoso. *Privacy Games Along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy*. ACM Trans. Priv. Secur., Vol. 19, Num. 4, pages 1–31, ACM, December 2016.

2. Isabel Garcia-Contreras, José F. Morales, Manuel Hermenegildo. *Semantic Code Browsing*. Theory and Practice of Logic Programming, 32nd International Conference on Logic Programming (ICLP'16) Special Issue, Vol. 16, Num. 5-6, pages 721–737, Cambridge U. Press, October 2016.

3. Pedro Lopez-Garcia, Maximilano Klemen, Umer Liqat, Manuel Hermenegildo. *A General Framework for Static Profiling of Parametric Resource Usage*. Theory and Practice of Logic Programming, 32nd International Conference on Logic Programming (ICLP'16) Special Issue, Vol. 16, Num. 5-6, pages 849–865, Cambridge U. Press, October 2016.

4. Manuel Carro, Andy King. *Introduction to the 32nd International Conference on Logic Programming Special Issue*. Theory and Practice of Logic Programming, Vol. 16, Num. 5-6, pages 509–514, Cambridge University Press, September 2016.

5. Veronica Mendoza, Richard Rivera, J.J. Barriga-Andrade. *Mobile Collaborative Learning Systems with Augmented Reality*. Revista Politécnica, Vol. 38, Num. 1, pages 71–80, Escuela Politécnica Nacional, September 2016.

6. Fredlund, Lars-Åke, Mariño, Julio, Alborodo, Raúl N.N., Herranz, Angel. *A testing-based approach to ensure the safety of shared resource concurrent systems*. Journal of Risk and Reliability, Proceedings of the Institution of Mechanical Engineers, Part O, Vol. 230, Num. 5, pages 457–472, Sage Publications, July 2016.

7. Juan Caballero, Zhiqiang Lin. *Type Inference on Executables*. ACM Computing Surveys, Vol. 48, Num. 4, pages 1–35, ACM, May 2016.

8. Roberto Giacobazzi, Isabella Mastroeni. *Making abstract models complete*. Mathematical Structures in Computer Science, Vol. 26, Num. 4, pages 658–701, Cambridge University Press, May 2016.

9. Javier Esparza, Pierre Ganty, Rupak Majumdar. *Parameterized Verification of Asynchronous Shared-Memory Systems*. J. ACM, Vol. 63, Num. 1, pages 1–48, ACM, March 2016.

10. Jeffrey Hughes, Cassandra Sparks, Alley Stoughton, Rinku Parikh, Albert Reuther, Suresh Jagannathan. *Building Resource Adaptive Software Systems (BRASS): Objectives and System Evaluation*. SIGSOFT Softw. Eng. Notes, Vol. 41, Num. 1, pages 1–2, ACM, January 2016.

11. José F. Morales, Manuel Carro, Manuel Hermenegildo. *Description and Optimization of Abstract Machines in a Dialect of Prolog*. Theory and Practice of Logic Programming, Vol. 16, pages 1–58, Cambridge University Press, January 2016.

12. Gilles Barthe, Juan Manuel Crespo, César Kunz. *Product programs and relational program logics*. J. Log. Algebr. Meth. Program., Vol. 85, Num. 5, pages 847–859, 2016.

13. Gilles Barthe, Marco Gaboardi, Justin Hsu, Benjamin C. Pierce. *Programming language techniques for differential privacy*. SIGLOG News, Vol. 3, Num. 1, pages 34–53, 2016.

14. Axel Schulz, Loza Mencía, Eneldo, Benedikt Schmidt. *A rapid-prototyping framework for extracting small-scale incident-related information in microblogs: Application of multi-label*

classification on tweets. Information Systems, Vol. 57, pages 88–110, 2016.

15. Simon Oya, Fernando Pérez-González, Carmela Troncoso. *Design of Pool Mixes Against Profiling Attacks in Real Conditions*. IEEE/ACM Trans. Netw., Vol. 24, Num. 6, pages 3662–3675, 2016.

16. Alejandro Sánchez, César Sánchez. *Parametrized Verification Diagrams: Temporal Verification of Symmetric Parametrized Concurrent Systems*. Annals of Mathematics and Artificial Intelligence, 2016.

17. Laura Bozzelli, César Sánchez. *Foundations of Boolean Stream Runtime Verification*. Theoretical Computer Science, Vol. 631, pages 118–138, 2016.

18. Bernd Finkbeiner, César Sánchez. *Special issue on Rich Models, EU-COST Action IC0901 Rich-Model Toolkit*. Acta Informatica, Vol. 53, Num. 4, pages 325–326, 2016.

19. César Sánchez, Kristen Brent Venable, Esteban Zimányi. *Special issue on temporal representation and reasoning (TIME'13)*. Acta Informatica, Vol. 53, Num. 2, pages 87–88, 2016.

20. Zorana Bankovic, Umer Liqat, Pedro Lopez-Garcia. *A General Methodology for Energy-efficient Scheduling in Multicore Environments based on Evolutionary Algorithms*. Journal of Multiple-Valued Logic and Soft Computing, SOCO'15 Special Issue, Old City Publishing, 2016.

21. Dario Catalano, Dario Fiore, Rosario Gennaro. *A Certificateless Approach to Onion Routing*. International Journal of Information Security, To Appear, Springer, 2016.

22. Giovanni Bernardi, Matthew Hennessy. *Using higher-order contracts to model session types*. Logical Methods in Computer Science, Vol. 12, Num. 2, 2016.

23. Guillermo Vigueras, Juan M. Orduña. *On the Use of GPU for Accelerating Communication-Aware Mapping Techniques*. The Computer Journal, Vol. 59, Num. 6, pages 836–847, 2016.

24. Kerstin Eder, John P. Gallagher, Pedro Lopez-Garcia, Henk L. Muller, Zorana Bankovic, Kyriakos Georgiou, Rémy Haemmerlé, Manuel Hermenegildo, Bishoksan Kafle, Steve Kerrison, Maja H. Kirkeby, Maximiliano Klemen, Xueliang Li, Umer Liqat, Jeremy Morse, Morten Rhiger, Mads Rosendahl. *ENTRA: Whole-systems energy transparency*. Microprocessors and Microsystems - Embedded Hardware Design, Vol. 47, pages 278–286, 2016.

25. Álvaro García-Pérez, Pablo. Nogueira. *No solvable lambda-value term left behind*. Logical Methods in Computer Science, Vol. 12, Num. 2, pages 1–43, 2016.

26. Antoine Durand-Gasselin, Javier Esparza, Pierre Ganty, Rupak Majumdar. *Model checking parameterized asynchronous shared-memory systems*. Formal Methods in System Design, pages 1–28, Springer, 2016.

27. Pierre Ganty, Radu Iosif, Filip Konecvčný. *Underapproximation of procedure summaries for integer programs*. International Journal on Software Tools for Technology Transfer, pages 1–20, Springer, 2016.

28. Javier Esparza, Pierre Ganty, Jérôme Leroux, Rupak Majumdar. *Verification of population protocols*. Acta Informatica, pages 1–25, Springer, 2016.

29. Julio Mariño, Raúl N.N. Alborodo, Angel Herranz, Lars-Åke Fredlund. *Synthesis of Verified Concurrent Java Components from Formal Models*. International Journal on Software and Systems Modeling, To Appear, Springer Berlin Heidelberg, 2016.

30. Isabella Mastroeni, Roberto Giacobazzi. *Weakening Additivity in Adjoining Closures*. Order, Vol. 33, Num. 3, pages 503–516, 2016.

31. Roberto Giacobazzi, Isabella Mastroeni, Mila Dalla Preda. *Maximal incompleteness as obfuscation potency*. Formal Aspects of Computing, To Appear, 2016.

32. Sandrine Blazy, Vincent Laporte, David Pichardie. *Verified Abstract Interpretation Techniques for Disassembling Low-level Self-modifying Code*. Journal of Automated Reasoning, Vol. 56, Num. 3, pages 283–308, 2016.

Conferences

1. Gilles Barthe, Marco Gaboardi, Emilio Jesús Gallego Arias, Justin Hsu, Aaron Roth, Pierre-Yves Strub. *Computer-aided verification in mechanism design*. Proceedings of the 12th Conference on Web and Internet Economics (WINE 2016), Springer-Verlag, December 2016. To appear.

2. Antonio Nappa, Rana Faisal Munir, Irfan Khan Tanoli, Christian Kreibich, Juan Caballero. *RevProbe: Detecting Silent Reverse Proxies in Malicious Server Infrastructures*. Proceedings of the 2016 Annual Computer Security Applications Conference, December 2016.

3. Joaquín Arias, Manuel Carro. *Description and Evaluation of a Generic Design to Integrate CLP and Tabled Execution*. 18th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'16), pages 10–23, ACM Press, September 2016.

4. Nataliia Stulova, José F. Morales, Manuel Hermenegildo. *Reducing the Overhead of Assertion Run-time Checks via Static Analysis*. 18th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'16), pages 90–103, ACM Press, September 2016.

5. Marcos Sebastián, Richard Rivera, Platon Kotzias, Juan Caballero. *AVClass: A Tool for Massive Malware Labeling*. Proceedings of the 19th International Symposium on Research in Attacks, Intrusions and Defenses, September 2016.

6. Alejandro Calleja, Juan Tapiador, Juan Caballero. *A Look into 30 Years of Malware Development from a Software Metrics Perspective*. Proceedings of the 19th International Symposium on Research in Attacks, Intrusions and Defenses, September 2016.

7. Platon Kotzias, Leyla Bilge, Juan Caballero. *Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services*. Proceedings of the 25th USENIX Security Symposium, August 2016.

8. Rémy Haemmerlé, Pedro Lopez-Garcia, Umer Liqat, Maximiliano Klemen, John P. Gallagher, Manuel Hermenegildo. *A Transformational Approach to Parametric Accumulated-cost Static Profiling*. 13th International Symposium on Functional and Logic Programming (FLOPS 2016), LNCS, Vol. 9613, pages 163–180, Springer, March 2016.

9. Ilya Sergey, Aleksandar Nanevski, Anindya Banerjee, Germán Andrés Delbianco. *Hoare-style Specifications As Correctness Conditions for Non-linearizable Concurrent Objects*. International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA), 2016.

10. Alberto Goffi, Alessandra Gorla, Michael D. Ernst, Mauro Pezzè. *Automatic Generation of Oracles for Exceptional Behaviors*. Proceedings of the 25th International Symposium on Software Testing and Analysis, ISSTA 2016, pages 213–224, ACM, 2016.

11. Hagit Attiya, Sebastian Burckhardt, Alexey Gotsman, Adam Morrison, Hongseok Yang, Marek Zawirski. *Specification and Complexity*

of Collaborative Text Editing. PODC'16: Symposium on Principles of Distributed Computing, pages 259–268, ACM Press, 2016.

12. Andrea Cerone, Alexey Gotsman. *Analysing Snapshot Isolation*. PODC'16: Symposium on Principles of Distributed Computing, pages 55–64, ACM Press, 2016.

13. Artem Khyzha, Alexey Gotsman, Matthew J. Parkinson. *A Generic Logic for Proving Linearizability*. FM'16: International Symposium on Formal Methods, LNCS, Vol. 9995, pages 426–443, Springer, 2016.

14. Giovanni Bernardi, Alexey Gotsman. *Robustness against Consistency Models with Atomic Visibility*. CONCUR'16: International Conference on Concurrency Theory, LIPICS, Vol. 59, pages 1–15, Dagstuhl, 2016.

15. Alexey Gotsman, Hongseok Yang, Carla Ferreira, Mahsa Najafzadeh, Marc Shapiro. *'Cause I'm strong enough: reasoning about consistency choices in distributed systems*. POPL'16: Symposium on Principles of Programming Languages, pages 371–384, ACM Press, 2016.

16. Torben Amtoft, Anindya Banerjee. *A Theory of Slicing for Probabilistic Control Flow Graphs*. Foundations of Software Science and Computation Structures - Proceedings of the 19th International Conference, FOSSACS 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, pages 180–196, 2016.

17. Anindya Banerjee, David A. Schmidt, Mohammad Nikouei. *Relational Logic with Framing and Hypotheses*. Proceedings of the 36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2016.

18. Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. *Proving Differential Privacy via Probabilistic Couplings*. Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2016, pages 749–758, ACM, 2016.

19. Gilles Barthe, Noémie Fong, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. *Advanced Probabilistic Couplings for Differential Privacy*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 55–67, ACM, 2016.

20. Gilles Barthe, Gian Pietro Farina, Marco Gaboardi, Emilio Jesús Gallego Arias, Andy Gordon, Justin Hsu, Pierre-Yves Strub. *Differentially Private Bayesian Programming*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 68–79, ACM, 2016.

21. Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini. *Strong Non-Interference and Type-Directed Higher-Order Masking*. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 116–129, ACM, 2016.

22. Gilles Barthe, Pedro R. D'Argenio, Bernd Finkbeiner, Holger Hermanns. *Facets of Software Doping*. Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications - Proceedings of the 7th International Symposium, ISoLA 2016, Part II, LNCS, Vol. 9953, pages 601–608, Springer, 2016.

23. José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir, Michael Emmi. *Verifying Constant-Time Implementations*. 25th USENIX Security Symposium, USENIX Security 16, pages 53–70, USENIX Association, 2016.

24. Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, Pierre-Yves Strub. *A Program Logic for Union Bounds*. 43rd International

Colloquium on Automata, Languages, and Programming, ICALP 2016, LIPIcs, Vol. 55, pages 1–15, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

25. Gilles Barthe, Thomas Espitau, Luis María Ferrer Fioriti, Justin Hsu. *Synthesizing Probabilistic Invariants via Doob's Decomposition*. Computer Aided Verification - Proceedings of the 28th International Conference, CAV 2016, Part I, LNCS, Vol. 9779, pages 43–61, Springer, 2016.

26. José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir. *Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC*. Fast Software Encryption - 23rd International Conference, FSE 2016, Revised Selected Papers, LNCS, Vol. 9783, pages 163–184, Springer, 2016.

27. Christian Meurisch, Usman Naeem, Muhammad Awais Azam, Frederik Janssen, Benedikt Schmidt, Max Mühlhäuser. *Smarticipation: intelligent personal guidance of human behavior utilizing anticipatory models*. Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp Adjunct 2016, pages 1227–1230, ACM, 2016.

28. Alexander Seeliger, Timo Nolle, Benedikt Schmidt, Max Mühlhäuser. *Process Compliance Checking using Taint Flow Analysis*. Proceedings of the International Conference on Information Systems - Digital Innovation at the Crossroads, ICIS 2016, Association for Information Systems, 2016.

29. Alexander Seeliger, Benedikt Schmidt, Immanuel Schweizer, Max Mühlhäuser. *What Belongs Together Comes Together: Activity-centric Document Clustering for Information Work*. Proceedings of the 21st International Conference on Intelligent User Interfaces, IUI 2016, pages 60–70, ACM, 2016.

30. Marc Fischlin, Felix Günther, Benedikt Schmidt, Bogdan Warinschi. *Key Confirmation in Key Exchange: A Formal Treatment and Implications for TLS 1.3*. IEEE Symposium on Security and Privacy, SP 2016, pages 452–469, IEEE Computer Society, 2016.

31. Raúl Pardo, Ivana Kellyerova, Cesar Sanchez, Gerardo Schneider. *Specification of Evolving Privacy Policies for Online Social Networks*. Proceedings of the 23rd Int'l Symp. on Temporal Representation and Reasoning (TIME'16), pages 70–79, IEEE Computer Society Press, 2016.

32. Dario Fiore, Cédric Fournet, Esha Gosh, Markulf Kohlweiss, Olga Ohrimenko, Bryan Parno. *Hash First, Argue Later: Adaptive Verifiable Computations on Outsourced Data*. ACM CCS 2016 – 23rd ACM Conference on Com-

puter and Communication Security, pages 1304–1316, 2016.

33. Dario Fiore, Aikaterini Mitrokotsa, Luca Nizzardo, Elena Pagnin. *Multi-Key Homomorphic Authenticators*. ASIACRYPT 2016: 22nd Annual International Conference on the Theory and Applications of Cryptology and Information Security, LNCS, Springer, 2016.

34. Dario Fiore, Anca Nitulescu. *On the (In) security of SNARKs in the Presence of Oracles*. TCC 2016-B: 14th Theory of Cryptography Conference, LNCS, Springer, 2016.

35. Johannes Krupp, Dominique Schroeder, Mark Simkin, Dario Fiore, Giuseppe Ateniese, Stefan Nuernberger. *Nearly Optimal Verifiable Data Streaming*. PKC 2016: 19th International Workshop on Theory and Practice in Public Key Cryptography, LNCS, Springer, 2016.

36. Bishoksan Kafle, John P. Gallagher, José F. Morales. *Rahft: A Tool for Verifying Horn Clauses Using Abstract Interpretation and Finite Tree Automata*. Computer Aided Verification - 28th International Conference, CAV 2016, Proceedings, Part I, LNCS, Vol. 9779, pages 261–268, Springer, 2016.

37. Xueliang Li, John P. Gallagher. *Fine-Grained Energy Modeling for the Source Code of a Mobile Application*. Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous 2016, pages 180–189, ACM, 2016.

38. Xueliang Li, John P. Gallagher. *A Source-level Energy Optimization Framework for Mobile Applications*. 16th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2016), 2016.

39. Michael Emmi, Constantin Enea. *Symbolic Abstract Data Type Inference*. Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, pages 513–525, ACM, 2016.

40. Miguel Ambrona, Gilles Barthe, Benedikt Schmidt. *Automated Unbounded Analysis of Cryptographic Constructions in the Generic Group Model*. Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS, Vol. 9666, pages 822–851, Springer, 2016.

41. Pavithra Prabhakar, Miriam García Soto, Ratan Lal. *Verification Techniques for Hybrid Systems*. Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications - 7th International Symposium, ISoLA 2016, Proceedings, Part II, pages 833–842, 2016.

42. Pavithra Prabhakar, Miriam García Soto. *An Algorithmic Approach to Global Asymptotic Stability Verification of Hybrid Systems*. Proceedings of the 13th International Conference on Embedded Software, EMSOFT 2016, pages 1–10, ACM, 2016.

43. Pavithra Prabhakar, Miriam García Soto. *Counterexample Guided Abstraction Refinement for Stability Analysis*. Computer Aided Verification - 28th International Conference, CAV 2016, LNCS, Vol. 9779, pages 495–512, Springer, 2016.

44. Pavithra Prabhakar, Miriam García Soto. *Hybridization for Stability Analysis of Switched Linear Systems*. Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, HSCC 2016, pages 71–80, ACM, 2016.

45. Javier Esparza, Pierre Ganty, Jérôme Leroux, Rupak Majumdar. *Model Checking Population Protocols*. 36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016), Leibniz International Proceedings in Informat-

ics (LIPIcs), Vol. 65, pages 1–14, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016.

46. Pierre Ganty, Damir Valput. *Bounded-oscillation Pushdown Automata*. Proceedings of the Seventh International Symposium on Games, Automata, Logics and Formal Verification, GandALF 2016, EPTCS, Vol. 226, pages 178–197, 2016.

47. Sophie Bernard, Yves Bertot, Laurence Rideau, Pierre-Yves Strub. *Formal proofs of transcendence for e and pi as an application of multivariate and symmetric polynomials*. Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs, pages 76–87, ACM, 2016.

48. Nikhil Swamy, Catalin Hritcu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cédric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, Jean Karim Zinzindohoue, Santiago Zanella Béguelin. *Dependent types and multi-monadic effects in F*. Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, pages 256–270, ACM, 2016.

49. Mila Dalla Preda, Roberto Giacobazzi, Isabella Mastroeni. *Completeness in Approximate Transduction*. Proceedings of the 23rd International Symposium on Static Analysis (SAS), LNCS, Vol. 9837, pages 126–146, Springer, 2016.

50. Sandrine Blazy, Vincent Laporte, David Pichardie. *An abstract memory functor for verified C static analyzers*. Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming, ICFP 2016, pages 325–337, 2016.

51. Cédric Fournet, Chantal Keller, Vincent Laporte. *A Certified Compiler for Verifiable Computing*. IEEE 29th Computer Security Foundations Symposium, CSF 2016, pages 268–280, 2016.

Workshops

1. Joaquín Arias. *Tabled CLP for Reasoning over Stream Data*. 12th ICLP Doctoral Consortium (DC-ICLP'16), pages 8, OASIcs, October 2016.

2. Jan Kuper, Lutz Schubert, Kilian Kempf, Colin Glas, Daniel Rubio Bonilla, Manuel Carro. *Program Transformations in the POLCA Project*. Design, Automation, and Testing in Europe, EDAA, March 2016.

3. Guillermo Vigueras, Manuel Carro, Salvador Tamarit, Julio Mariño. *Towards Automatic Learning of Heuristics for Mechanical Transformations of Procedural Code*. Proceedings of the First International Workshop on Program Transformation for Programmability in Heterogeneous Architectures (PROHA 2016), March 2016.

4. Salvador Tamarit, Julio Mariño, Guillermo Vigueras, Manuel Carro. *Towards a Semantics-Aware Transformation Toolchain for Heterogeneous Systems*. Proceedings of the First International Workshop on Program Transformation for Programmability in Heterogeneous Architectures (PROHA 2016), March 2016.

5. Konstantin Kuznetsov, Vitalii Avdiienko, Alessandra Gorla, Andreas Zeller. *Checking App User Interfaces Against App Descriptions*. Proceedings of the 1st International Workshop on App Market Analytics, WAMA 2016, pages 1–7, ACM, 2016.

6. Vitalii Avdiienko, Konstantin Kuznetsov, Paolo Calciati, Juan Carlos Caiza Román, Alessandra Gorla, Andreas Zeller. *CALAPPA: a Toolchain for Mining Android Applications*. Proceedings of the 1st International Workshop on App Market Analytics, WAMA 2016, pages 22–25, ACM, 2016.

7. Mahsa Najafzadeh, Alexey Gotsman, Hongseok Yang, Carla Ferreira, Marc Shapiro. *The CISE tool: proving weakly-consistent applications correct*. PAPOC'16: Workshop on the Principles and Practice of Consistency for Distributed Data, pages 1–3, ACM Press, 2016.

8. Jamie Hayes, Carmela Troncoso, George Danezis. *TASP: Towards Anonymity Sets that Persist*. 15th Workshop on Privacy in the Electronic Society, WPES, ACM, 2016.

9. Umer Liqat, Zorana Bankovic, Pedro Lopez-Garcia, Manuel Hermenegildo. *Inferring Energy Bounds Statically by Evolutionary Analysis of Basic Blocks*. Workshop on High Performance Energy Efficient Embedded Systems (HIP3ES 2016), 2016. arXiv:1601.02800.

10. Bishoksan Kafle, John P. Gallagher. *Interpolant tree automata and their application in Horn clause verification*. Proceedings of the Fourth International Workshop on Verification and Program Transformation, VPT 2016, Eindhoven, The Netherlands, 2nd April 2016., EPTCS, Vol. 216, pages 104–117, 2016.

11. Bishoksan Kafle, John P. Gallagher, Pierre Ganty. *Solving non-linear Horn clauses using a linear Horn clause solver*. Proceedings 3rd Workshop on Horn Clauses for Verification and Synthesis, HCVS 2016, satellite event of ETAPS, Eindhoven, The Netherlands, 3rd April 2016, EPTCS, Vol. 219, pages 33–48, 2016.

6.1.2. Edited Volumes

1. Manuel Carro, Andy King (Eds.). *32nd International Conference on Logic Programming*. Vol. 16, Num. 5-6, Cambridge University Press, September 2016.

2. Manuel Carro, Salvador Tamarit, Guillermo Vigueras, Julio Mariño (Eds.). *First International Workshop on Program Transformation for Programmability in Heterogeneous Architectures (PROHA 2016)*. March 2016.

3. Ayal Zaks, Manuel Hermenegildo. *Proceedings of the 25th International Conference on Compiler Construction (CC 2016)*. ACM, March 2016.

4. Gilles Barthe, Evangelos P. Markatos, Pierangela Samarati (Eds.). *Security and Trust Management - 12th International Workshop, STM 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings*. LNCS, Vol. 9871, Springer, 2016.

5. Manuel Carro, Andy King, Neda Saeedloei, Marina De Vos (Eds.). *Technical Communications of the 32nd International Conference on Logic Programming*. OASICS, Vol. 52, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

6. John P. Gallagher, Philipp Rümmer (Eds.). *Proceedings 3rd Workshop on Horn Clauses for Verification and Synthesis, HCVS (satellite event of ETAPS), Eindhoven, The Netherlands, 3rd April 2016*. EPTCS, Vol. 219, 2016.

7. Juan Caballero, Urko Zurutuza, Ricardo J. Rodríguez. *Detection of Intrusions and Malware, and Vulnerability Assessment - 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings*. LNCS, Vol. 9721, Springer, 2016.

8. Juan Caballero, Eric Bodden, Elias Athanasopoulos. *Engineering Secure Software and*

Systems - 8th International Symposium, ESSoS 2016. Proceedings. LNCS, Vol. 9639, Springer, 2016.

9. Pierre Ganty, Michele Loreti (Eds.). *Trustworthy Global Computing - 10th International Symposium, TGC 2015, Madrid, Spain, August 31 - September 1, 2015, Revised Selected Papers*. LNCS, Vol. 9533, Springer, 2016.

6.1.3. Articles in Books and other Collections

1. Umer Liqat, Kyriakos Georgiou, Steve Kerrison, Pedro Lopez-Garcia, Manuel Hermenegildo, J. P. Gallagher, Kerstin Eder. *Inferring Parametric Energy Consumption Functions at Different Software Levels: ISA vs. LLVM IR*. Foundational and Practical Aspects of Resource Analysis: 4th International Workshop, FOPARA 2015. Revised Selected Papers, LNCS, Vol. 9964, pages 81–100, Springer, 2016.

6.1.4. Doctoral, Master and Bachelor Theses

1. Juan Manuel Crespo. *Automation and Modularity of Cryptographic Proofs in the Computational Model*. Ph.D. Thesis. Technical University of Madrid (UPM). May 2016. Advisor: Gilles Barthe (IMDEA Software Institute).

2. Goran Doychev. *Tools for the Evaluation and Choice of Countermeasures against Side-channel Attacks*. Ph.D. Thesis. Technical University of Madrid (UPM). May 2016. Advisor: Boris Koepf (IMDEA Software Institute).

3. Antonio Nappa. *Defending Against Cybercrime: Advances in the Detection of Malicious Servers and the Analysis of Client-Side Vulnerabilities*. Ph.D. Thesis. Technical University of Madrid (UPM). February 2016. Advisor: Juan Caballero (IMDEA Software Institute).

4. Isabel Garcia. *Code Search: A Semantic, Abstract Interpretation-Based Approach*. M.Sc. Thesis. Technical University of Madrid (UPM). July 2016. Advisors: Manuel Hermenegildo and José F. Morales (IMDEA Software Institute).

5. Alexander Schramm. *An Asynchronous Evaluation Engine for Stream Based Specifications*. M.Sc. Thesis. Universitat zu Luebeck, Germany. December 2016. Advisor: Cesar Sanchez (IMDEA Software Institute).

6. Hasser Verramendi. *Privacy Implications of Open Data*. M.Sc. Thesis. Technical University of Madrid (UPM). July 2016. Advisor: Carmela Troncoso (IMDEA Software Institute).

7. Victor de Juan. *Pruebas de Primer Orden de Programas Concurrentes*. Bachelor Thesis. Universidad Autonoma de Madrid (UAM). July 2016. Advisor: Cesar Sanchez (IMDEA Software Institute).

8. Elena Gutierrez. *Linearisation of k-index bounded sets of Horn clauses*. Bachelor Thesis. Universidad Autonoma de Madrid (UAM). May 2016. Advisor: Pierre Ganty (IMDEA Software Institute).

9. Alejandro Ranchal Pedrosa. *Implementing Fully Homomorphic Encryption Schemes in FPGA-based Systems*. B.Sc. Thesis. Technical University of Madrid (UPM). January 2016. Advisor: Manuel Carro (IMDEA Software Institute).

10. Pedro Valero. *Languages and Security*. Bachelor Thesis. Universidad Autonoma de Madrid (UAM). May 2016. Advisors: Pierre Ganty and Boris Koepf (IMDEA Software Institute).

6.2. Invited Talks

6.2.1. Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Computer-Aided Cryptography. Invited talk at the 28th International Conference on Computer Aided Verification (CAV 2016). Toronto, Ontario, Canada. July 2016.

2. *Gilles Barthe*. Verification of differential private computations. Invited talk at the International Joint Conference on Automated Reasoning (IJCAR 2016). Coimbra, Portugal. July 2016.

3. *Juan Caballero*. CyberProbe & AutoProbe: Towards Internet-Scale Active Detection of Malicious Server. Invited talk at GSE Management Forum. Lisbon, Portugal. September 2016.

4. *Manuel Carro*. Towards Automatic Learning of Heuristics for Mechanical Transformations of Procedural Code. Invited talk at the HiPEAC SW_ENG (Software Engineering; Programming Future Large Scale IT Systems) workshop. Prague, Czeck Republic. January 2016.

5. *François Dupressoir*. Formal and Compositional Proofs of Probing Security for Masked Algorithms. Invited Talk at the 7th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2016). Graz, Austria. April 2016.

6. *Dario Fiore*. Modern Cryptography for Privacy and Integrity in the Cloud. Invited talk at GSE Management Summit, Lisbon, Portugal. September 2016.

7. *Dario Fiore*. Secure Outsourcing of Data and Computation to the Cloud. Invited talk at EIT Digital Symposium: security of digital systems and protocols, Rennes, France. November 2016.

8. *Pierre Ganty*. Working the crowd. Invited keynote at the Microsoft Research – IMDEA Software Institute Collaborative Workshop, Cambridge, UK, June 2016.

9. *John Gallagher*. Finite Tree Automata in Horn Clause Transformations. Invited talk at the 4th International Workshop on Verification and Program Transformation. April 2016.

10. *Boris Koepf*. Reasoning about the Trade-off between Security and Performance. Invited keynote at Workshop on Safety and Security Assurance for Critical Infrastructure Protection (S4CIP). Madrid, Spain. May 2016.

6.2.2. Invited Seminars and Lectures by IMDEA Scientists

1. *Miguel Ambrona*. Automated Unbounded Analysis of Cryptographic Constructions in the Generic Group Model. Cryptography Seminars Day at URJC, Madrid, Spain. September 2016.

2. *Miguel Ambrona*. Generic Transformations of Predicate Encodings: Constructions and Applications. Invited seminar at École Normale Supérieure, Paris, France. November 2016.

3. *Andrea Cerone*. Analyzing Transactional Consistency Models. Invited talk at Microsoft Research, Cambridge, UK. January 2016.

4. *Andrea Cerone*. Analyzing Transactional Consistency Models. Invited talk at University of Kent, Canterbury, UK. January 2016.

5. *Andrea Cerone*. Analyzing Transactional Consistency Models. Invited talk at Imperial College, London, UK. January 2016.

6. *Andrea Cerone*. Analyzing Snapshot Isolation. Workshop on Principles and Practice of Consistency for Distributed Data (PaPoC 2016), London, UK. April 2016.

7. *Germán Andrés Delbianco*. Concurrent Data Structures Linked in Time. VT Seminars – Com-

puter Science Department, University of Sheffield. Sheffield, UK. May 2016.

8. *Dario Fiore*. ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data. CryptoAction Symposium, Budapest, Hungary. April 2016.

9. *Dario Fiore*. Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data. Cryptography Seminars Day at URJC, Madrid, Spain. September 2016.

10. *Miriam García*. An algorithmic approach to global asymptotic stability verification of hybrid systems. Invited talk at Dagstuhl Seminar "Robustness in Cyber-Physical Systems" (16362), Schloss Dagstuhl, Germany, September 2016.

11. *Alessandra Gorla*. Automatic Generation of Oracles for Exceptional Behaviors. Invited talk at University of Luxembourg. April 2016.

12. *Alessandra Gorla*. Mining Android Apps for Anomalous Behavior. Invited talk at University of Washington, Seattle, USA. November 2016.

13. *Boris Koepf*. Static Analysis of Cache Side Channels. Invited talk at FireEye, Dresden, Germany. April 2016.

14. *Boris Koepf*. Reasoning about the Trade-off between Security and Performance. Invited talk at TU Dresden, Germany. April 2016.

15. *Boris Koepf*. Reasoning about the Trade-off between Security and Performance. Invited talk at CNR, Pisa, Italy. September 2016.

16. *Boris Koepf*. Reasoning about the Trade-off between Security and Performance. Invited talk at University of Florence, Italy. September 2016.

17. *Boris Koepf*. Static Quantification of Side Channel Leaks. Invited talk at TU Darmstadt, Germany. December 2016.

18. *Boris Koepf*. Statische Quantifizierung von Seitenkanälen in Softwaresystemen. Invited talk at University of the Armed Forces, Munich, Germany. December 2016.

19. *Artem Khyzha*. Proving Linearizability Using Partial Orders. Kent Concurrency Workshop, University of Kent, Canterbury, UK. July 2016.

20. *Aleks Nanevski*. Separation Logic and Concurrency. Invited lectures at the Oregon Programming Languages Summer School (OPLSS 2016). University of Oregon, USA. July 2016.

21. *Pablo Nogueira*. Sin dejarse atrás términos lambda-valor resolubles. Universidad Complutense de Madrid. July 2016.

22. *Benedikt Schmidt*. Computer-Aided Game-Based Proofs. Invited lecture at Summer School on Computer Aided Analysis of Cryptographic Protocols, Bucharest, Romania. September 2016.

23. *Carmela Troncoso*. Traffic analysis: or... encryption is not enough. Invited lecture at Summer Research Institute. Security/Privacy Edition. Laussane, Switzerland. June 2016.

24. *Carmela Troncoso*. Traffic analysis: or... encryption is not enough. Invited lecture at Summer school on real-world crypto and privacy. Sibenik, Croatia. June 2016.

25. *Carmela Troncoso*. Introduction to Privacy. Invited lecture at Intensive Programme on Information and Communication Systems Security (IPICS 2016). Leuven, Belgium. July 2016.

6.2.3. Invited Speaker Series

During 2016, 30 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. *Pablo Picazo-Sanchez*. Ph.D. Student, Ph.D. Student, Universidad Carlos III, Spain: Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Networks.

2. *Jacques-Henri Jourdan*. Ph.D. Student, INRIA, France: Verasco: A Formally Verified C Static Analyzer.

3. *Fernando Pérez González*. Full Professor, University of Vigo, Spain: Adversarial Signal Processing.

4. *Adam Morrison*. Postdoctoral Researcher, Technion - Israel Institute of Technology, Israel: Limitations of Highly-Available Eventually-Consistent Data Stores.

5. *Reynald Affeldt*. Senior Research Scientist, National Institute of Advanced Industrial Science and Technology, Japan: Formalization of Error-correcting Codes: from Hamming to Modern Coding Theory.

6. *Hugo Krawczyk*. Research Scientist, IBM T. J. Watson Research Center, USA: Protecting our Protectors: Armoring Passwords Against Server Compromise (Or: How to Protect Your Bitcoin Wallet Online).

7. *Reinhard Wilhelm*. Professor, Saarland University, Germany: Toward Compact Abstract Domains for Pipelines.

8. *Aishwarya Thiruvengadam*. Ph.D. Student, University of Maryland, USA: 10-round Feistel is indifferentiable from an ideal cipher.

9. *Christopher Meiklejohn*. Ph.D. Student, KU Leuven, Belgium: Lasp: A Language For Distributed, Declarative, Edge Computation.

10. *Patrick Cousot*. Full Professor, New York University: The hierarchy of analytic semantics of weakly consistent parallelism.

11. *Alessio Gambi*. Post-doctoral Researcher, Saarland University, Germany: O!Snap: Cost-Efficient Testing in the Cloud.

12. *Jens Grossklags*. Assistant Research Professor, University of Pennsylvania, USA: Given Enough Eyeballs, All Bugs Are Shallow? An Empirical Study of the Wooyun and HackerOne Web Vulnerability Discovery Ecosystems.

13. *Toby Murray*. Lecturer, The University of Melbourne, Australia: Building Highly-Secure Systems at Reasonable Cost – Branching Out with Formal Verification.

14. *Peter Stuckey*. Professor, The University of Melbourne, Australia: Optimization Modelling for Software Developers, or How to convert procedural code to constraints!

15. *Wouter Lueks*. Ph.D. Student, University of Nijmegen, Netherlands: Distributed encryption and applications.

16. *Antonio Faonio*. Post-doctoral Researcher, Aarhus University, Denmark: Fully Leakage-Resilient Signatures with Graceful Degradation.

17. *Michael Pradel*. Research Group Leader, TU Darmstadt, Germany: Scalable Program Analyses for JavaScript-based Web Applications.

18. *Svetlana Jakšić*. Ph.D. Student, University of Novi Sad, Serbia: Types for Privacy and Memory Control.

19. *Yuri Meshman*. Ph.D. Student, Technion - Israel Institute of Technology, Israel: Pattern-based Synthesis of Synchronization for the C++ Memory Model.

20. *Mooly Sagiv*. Professor, Tel Aviv University, Israel: Ivy: Safety Verification by Interactive Generalization.

21. *Jesús Díaz Vico*. Research Scientist, BEEVA, Spain: Anonymization and De-anonymization: With Great Power Comes Great Responsibility... or not?

22. *Valter Balegas*. Ph.D. Student, Universidade Nova de Lisboa, Portugal: IPA: Invariant-Preserving Applications for Weakly-consistent Replicated Databases.

23. *Matthieu Perrin*. Post-doctoral Researcher, Technion - Israel Institute of Technology, Israel: Specification of shared objects in wait-free distributed systems.

24. *Narseo Vallina-Rodriguez*. Assistant Research Professor and Research Scientist, IMDEA Networks, Spain and International Computer Science Institute (ICSI), USA: The ICSI Haystack: A Tool to Illuminate the Mobile Ecosystem.

25. *Francesco Zappa Nardelli*. Research Scientist, INRIA Paris, France: Programming Languages and Concurrency: Still Tricky

26. *Antonio Nappa*. Research Scientist, Stealth-Sec Inc., España: RevProbe: Detecting Silent Reverse Proxies in Malicious Server Infrastructures.

27. *Daniel Larraz*. Ph.D. Researcher, Universitat Politècnica de Catalunya (UPC), Spain: Scalable Program Analysis using Max-SMT.

28. *Avinash Sudhodanan*. Junior researcher, Fondazione Bruno Kessler, Italy: Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications.

29. *Fernando Pedone*. Professor, Università della Svizzera Italiana, Lugano, Switzerland: Scaling State Machine Replication.

30. *Emanuele D'Osualdo*. Post-doctoral Researcher, TU Kaiserslautern, Germany: Automatic Analysis of Message Passing Concurrency.

6.2.4. Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of **20** seminars were given in 2016.

6.3. Scientific Service and Other Activities

6.3.1. Conference and Program Committee Chairmanship

Gilles Barthe:

1. PC Co-chair of the 12th International Workshop on Security and Trust Management (STM 2016).

Juan Caballero:

2. PC Co-chair of the 8th International Symposium on Engineering Secure Software and Systems (ESSoS 2016).

3. PC Chair of the 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2016).

Manuel Carro:

4. PC Co-chair of the 32nd International Conference on Logic Programming (ICLP 2016).

5. Co-organizer of the 1st International Workshop on Program Transformation for Programmability in Heterogeneous Architectures (PROHA 2016).

John Gallagher:

6. PC Co-chair of the 3rd Workshop on Horn Clauses for Verification and Synthesis (HCVS 2016).

Alessandra Gorla:

7. Artifact Evaluation co-chair, ACM International Symposium on Software Testing and Analysis (ISSTA 2016).

8. Artifact Evaluation co-chair, International Symposium on Engineering Secure Software and Systems (ESSoS 2016).

9. Tool Demonstrations co-chair, 24th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2016).

Manuel Hermenegildo:

10. PC Chair of the 25th International Conference on Compiler Construction (CC 2016).

11. PC Chair of the 26th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2016).

Boris Koepf:

12. PC Co-chair of the 29th IEEE Computer Security Foundations Symposium (CSF 2016).

Pedro Lopez:

13. PC Chair of the 26th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2016).

Cesar Sanchez:

14. PC Co-chair of the 16th International Conference on Runtime Verification (RV 2016).

Carmela Troncoso:

15. Award Chair of PET 2016.

6.3.2. 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. Steering committee of IEEE European Symposium on Security and Privacy (Euro S&P).

4. Steering committee of the European Joint Conferences on Theory and Practice of Software (ETAPS).

Juan Caballero:

5. Editorial Board of the ACM Transactions in Privacy and Security (ACM TOPS).

6. Steering committee of Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).

7. Steering committee of Jornadas Nacionales de Investigación en Ciberseguridad (JNIC).

8. Steering Committee of the International Symposium on Engineering Secure Software and Systems (ESSoS).

Dario Fiore:

9. Editorial board of IET Information Security.

John Gallagher:

10. Editorial board of Theory and Practice of Logic Programming (Cambridge Univ. Press). Area Editor for Technical Notes and Rapid Publications.

Alexey Gotsman:

11. Steering committee of Workshop on Principles and Practice of Consistency for Distributed Data (PaPoC), affiliated with EuroSys.

Manuel Hermenegildo:

12. Steering Committee of the Static Analysis Symposium (SAS).

13. Steering Committee of the International Symposium on Functional and Logic Programming (FLOPS).

14. Steering Committee of the International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI).

15. Steering Committee of the Conference on Compiler Construction (CC).

16. Editorial Advisor and former Area Editor (architecture and implementation) of "Theory and Practice of Logic Programming" (Cambridge U. Press)

17. Associate Editor of the "Journal of New Generation Computing" (Springer-Verlag)

18. Area Editor of "Journal of Applied Logic" (Elsevier North-Holland).

19. Area Editor, Algorithms in Programming Languages and Software Engineering, of the "Journal of the IGPL" (Oxford U press).

Boris Koepf:

20. Steering committee of IEEE Computer Security Foundations Symposium (CSF).

21. Steering committee of ETAPS Conference on Principles of Security and Trust (POST).

22. Steering committee of Workshop on Foundations of Computer Security (FCS).

Pablo Nogueira:

23. Steering Committee of the International Conference on Mathematics of Program Construction.

24. Steering committee of Spanish EDINF Working Group (computer science education under 18).

6.3.3. Participation in Program Committees

Gilles Barthe:

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

2. 21st International Symposium on Formal Methods (FM 2016).

Giovanni Bernardi:

3. 9th Interaction and Concurrency Experience (ICE 2016).

Juan Caballero:

4. 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016).

5. 25th USENIX Security Symposium (USENIX Security 2016).

6. 16th International Conference on Runtime Verification (RV 2016).

7. 11th Symposium on Electronic Crime Research (eCrime 2016).

8. 11th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016).

Manuel Carro:

9. 14th International Conference on Service Oriented Computing (ICSOC 2016).

10. 18th International Symposium on Practical Aspects of Declarative Languages (PADL 2016).

Dario Fiore:

11. 19th International Conference on Practice and Theory in Public Key Cryptography (PKC 2016).

12. 35th Annual Eurocrypt Conference (EUROCRYPT 2016).

13. 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016).

14. 1st IEEE European Symposium on Security and Privacy (EuroS&P 2016).

15. 8th International Conference on Cryptology (Africacrypt 2016).

16. 3rd Annual International Conference on Cryptography and Information Security (BalkanCryptSec 2016).

17. 31st ACM Symposium on Applied Computing – Security Track (ACM SEC@SAC 2016).

John Gallagher:

18. 32nd International Conference on Logic Programming (ICLP 2016).

19. 28th Nordic Workshop on Programming Theory (NWPT 2016).

Pierre Ganty:

20. 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2016).

21. 23rd International Static Analysis Symposium (SAS 2016).

22. 12th Summer School on Modelling and Verification of Parallel Systems (MOVEP 2016).

23. 3rd Workshop on Horn Clauses for Verification and Synthesis (HCVS 2016).

Alessandra Gorla:

24. 6th Software Security, Protection, and Reverse Engineering Workshop (SSPREW 2016).

25. 8th Symposium on Search Based Software Engineering (SSBSE 2016).

26. 32nd IEEE International Conference on Software Maintenance and Evolution (ICSME 2016), Tool Demos Track

27. 13th Working Conference on Mining Software Repositories (MSR 2016).

28. ACM International Symposium on Software Testing and Analysis (ISSTA 2016).

29. IEEE International Conference on Software Testing, Verification and Validation (ICST 2016).

30. IEEE/ACM Third International Conference on Mobile Software Engineering and Systems (MOBILE-Soft 2016).

31. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2016), Visions of 2025 and Beyond Track.

32. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2016) Workshops.

33. 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016), ERA Track.

34. 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016).

35. 31st Annual ACM/SIGAPP Symposium On Applied Computing (SAC 2016), Service-Oriented Architectures and Programming (SOAP) Track 2016.

Alexey Gotsman:

36. Workshop on Programming Models and Languages for Distributed Computing (PMLDC 2016).

37. 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. (POPL 2016).

38. 27th International Conference on Concurrency Theory (CONCUR 2016).

Manuel Hermenegildo:

39. 37th annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI 2016).

40. Workshop on Application of Logic Programming (AppLP 2016).

Boris Koepf:

41. 1st IEEE Conference on Cybersecurity Development (SecDev 2016).

42. 4th Workshop on Hot Issues in Security Principles and Trust (HotSpot 2016).

Srdjan Matic:

43. Artifact evaluation committee of the International Symposium on Software Testing and Analysis (ISSTA 2016).

José Morales:

44. 32nd International Conference on Logic Programming (ICLP 2016).

45. Artifact evaluation committee of the 37th annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI 2016).

46. 25th International Conference on Compiler Construction (CC 2016).

Aleks Nanevski:

47. International Joint Conference on Automated Reasoning (IJCAR 2016).

48. 21st ACM SIGPLAN International Conference on Functional Programming (ICFP 2016).

Pablo Nogueira:

49. Workshop Educación en Informática (EI<18).

Cesar Sanchez:

50. XVI Jornadas sobre Programación y Lenguajes (PROLE 2016).

51. 14th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS 2016).

52. 12th International Conference on integrated Formal Methods (iFM 2016).

Peter Stuckey:

53. 13th International Conference on Integration of Artificial Intelligence and Operations Research (OR) techniques in Constraint Programming (CPAIOR 2017).

54. 31st National Conference on Artificial Intelligence (AAAI 2017).

55. 22nd International Conference on Principles and Practice of Constraint Programming 2016 (CP2016).

Carmela Troncoso:

56. 37th IEEE Symposium on Security and Privacy (S&P 2016).

57. II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016).

6.3.4. Association and Organization Committees

Miguel Ambrona:

1. Co-organizer of the Workshop on Cryptography and Internet Security, Semana de la Ciencia Complutense, Universidad Complutense, Madrid, Spain.

Gilles Barthe:

2. Organizing committee of the International School on Foundations of Security Analysis and Design (FOSAD).

Manuel Carro:

3. Representative of UPM in ERCIM.

4. Deputy representative of IMDEA Software in Informatics Europe.

5. Conference coordinator of the Association for Logic Programming.

Dario Fiore:

6. Vice-chair of COST Action IC1306 "Cryptography for Secure Digital Interaction."

7. Organizing committee of CryptoAction Symposium, Budapest, Hungary. April 2016.

Manuel Hermenegildo:

8. Director, EIT Digital Madrid Associate Partner Group.

9. Vice-President of Informatics Europe. Member Informatics Europe department evaluation board.

10. Elected President of SpaRCIM, the Spanish Research Consortium for Informatics and Mathematics (Spain's ERCIM member).

11. Member of INRIA scientific council (Institut National de Recherche en Informatique et en Automatique, France).

12. Member *Academia Europaea*.

13. Member of Schloss Dagstuhl scientific advisory board.

14. Member IRILL (French Institute for Free Software) scientific advisory board.

15. Member of the External Advisory Board of the NOVA LINCS Institute (Portugal).

16. Secretary of the International Association for Logic Programming.

17. Member of the International Federation for Computational Logic (IFCoLog) Advisory Board.

Pablo Nogueira:

18. Organizing Committee of Workshop Educación en Informática (EI<18).

Cesar Sanchez:

19. Local Organizing Committee of the 16th International Conference on Runtime Verification, Madrid, Spain. September 2016.

Carmela Troncoso:

20. Editorial Board Proceedings on Privacy Enhancing Technologies (PoPETs).

21. Steering Committee of Privacy Enhancing Technologies Symposium (PETS).

22. ERCIM STM 2016 Ph.D. Thesis Award Committee.

Guillermo Vigueras:

23. Organization Committee of the First International Workshop on Program Transformation for Programmability in Heterogeneous Architectures (PROHA 2016).

6.4. Awards

Conference Paper Awards:

1. J. B. Almeida, M. Barbosa, *G. Barthe*, and *F. Dupressoir*. Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC. The 23rd International Conference on Fast Software Encryption (FSE 2016). **Best paper award**.

2. *A. Cerone*, and *A. Gotsman*. Analysing snapshot isolation. The 36th ACM Symposium on Principles of Distributed Computing (PODC 2016). **Best paper award**.

3. V. Avdiienko, K. Kuznetsov, *A. Gorla*, A. Zeller, S. Arzt, S. Rasthofer, and E. Bodden. Abnormal Sensitive Data Usage in Android Apps. II Jornadas Nacionales de Investigacion en Ciberseguridad (JNIC 2016). **Special mention.**

4. *N. Stulova, J. F. Morales, M. V. Hermenegildo.* Reducing the Overhead of Assertion Run-time Checks via Static Analysis. 18th Int'l. ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'16), pages 90-103, ACM Press, September 2016. **Highest ranked paper.**

Other Awards:

5. M. Backes, M. Barbosa, *D. Fiore*, and R. M. Reischuk. ADSNARK: nearly practical and privacy-preserving proofs on authenticated data. **2016 CNIL-Inria Award for Privacy Protection**.

6. *Carmela Troncoso.* 37th IEEE Symposium on Security and Privacy (S&P 2016). **Best reviewer award**.

7. *Alejandro Sanchez*: **UPM Doctoral Outstanding Award** 2014/2015 (awarded in 2016).

6.5. Dissemination Events

In 2015 IMDEA Software researchers have participated in a number of events related to dissemination and the promotion of science.

Researcher's Night. In September 2016, as in previous years, the IMDEA Software Institute participated in the European-wide initiative "Researchers' Night". This year, its unifying topic was "*Sporty Science or Sciencefull Sport*": taking their field of expertise as starting point, researchers from the IMDEA Institutes were interviewed to show that science and sports, despite their apparent differences, have many points in common. Science has of course contributed to sports from many angles and many characteristics of sports appear in science and scientific work: continuous improvement and teamwork are essential, competition is fierce, and honor and respect for the colleagues are universally regarded as prime values. IMDEA Software Institute researchers Manuel Carro (Deputy Director) and César Sánchez (Associate Research Professor) took part in the event as host and one of the interviewees.

Full description:
http://www.imdea.org/events/imdea-initiative/2016/sporty-science-or-sciencefull-sport-european-researchers-night-madrid

Industrial and Entrepreneurship-Oriented Events. In addition to all the forms of transfer and collaboration mentioned before (from research projects with industrial partners committed to the commercial exploitation of results to all the activities of the Spanish associate node of EIT Digital, significant accelerators of such transfer), important additional missions are to disseminate results and to create awareness of the return on investment of research. To this end, the Institute organizes and participates in a wide range of industrial and entrepreneurship-oriented events, which in 2016 included the following:

1. EIT Digital/UPM: Entrepreneurship course on Opportunity Recognition. February 206.
2. EIT Digital/UPM: Data Science Master Welcome Day. September 2016.
3. EIT Digital: Digital Infrastructure meeting with demonstration of Cloud innovation activities. September 2016
4. EIT Digital: Raising I&E Awareness. October 2016.
5. EIT Digital: Cybersecurity Matchmaking event. November 2016.

scientific highlights

annual report 2016

a rigorous

A Rigorous Approach to Consistency in Cloud Databases

The past decade has witnessed a spectacular growth of cloud-based Internet services. Web sites such as Amazon and Facebook process hundreds of thousands of user requests per second, yet stay available at all times. To achieve this, the shared data accessed by the requests is managed by novel *cloud databases*, which partition and replicate the data across a large number of nodes and/or a wide geographical span. To achieve high availability and scalability, cloud databases need to maximise the parallelism of data processing. Unfortunately, this leads them to weaken the guarantees they provide about data consistency to applications. The resulting programming models are very challenging to use correctly, and we currently do not have advanced methods and tools that would help programmers in this task.

The goal of the 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. Our theory will then serve as a basis for practical implementation techniques and tools that harness database parallelism, but only to the extent such that the side effects of the parallelism do not compromise application correctness. This is a rigorous approach to the problem of data consistency in cloud databases that aims to push the envelope in their availability, scalability and cost-effectiveness.

The mathematical models and reasoning methods developed in the project will enable programming language and verification researchers to further improve the quality of applications using cloud databases. By applying the theory of cloud databases to their implementations, the project will also allow systems researchers to design these databases in a more principled way, informed by the consistency requirements of applications using them. Finally, the project will address a pressing need of the software industry

to consistency in cloud databases

approach

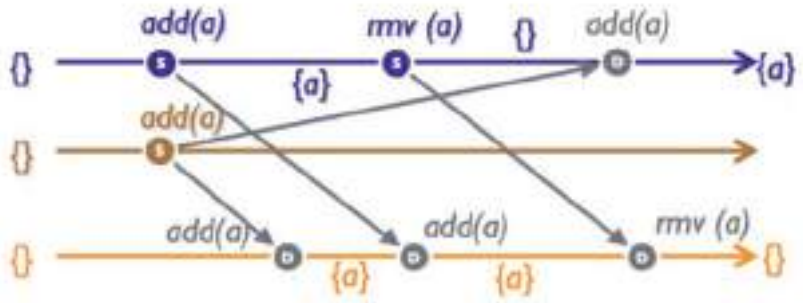
for systematic techniques to scalably manage data consistency. The rigorous approach promoted by the project can facilitate constructing large-scale services that are correct, yet maximally exploit the parallelism enabled by cloud computing. Increased parallelism will allow achieving better availability and scalability with fewer resources, thus lowering costs and helping the industry cope with ever growing pressures on its infrastructure. In the end, these technological advances will benefit the society as a whole, by enabling more reliable and affordable Internet services that all of us use every day.

The research in the above project is supported by an ERC Starting Grant RACCOON held by Alexey Gotsman during 2017-2021.

Related publications

[1] *Alexey Gotsman*, Hongseok Yang, Carla Ferreira, Mahsa Najafzadeh, and Marc Shapiro. 'Cause I'm strong enough: reasoning about consistency choices in distributed systems. POPL'16: Symposium on Principles of Programming Languages, St. Petersburg, FL, USA, pages 371-384. ACM, 2016.

[2] *Andrea Cerone* and *Alexey Gotsman*. Analysing snapshot isolation. PODC'16: Symposium on Principles of Distributed Computing, Chicago, IL, USA, pages 55-64. ACM, 2016.



type and proof

Type and Proof Structures for Concurrent Software Verification

Chip manufacturers today have reached, due to thermal limits and other considerations, processing speed ceilings for computer processors. This leaves concurrent programming, where one program executes on many processors, as the only way to scale our computing power.

Unfortunately, concurrent programs are notoriously difficult to write because of the complexity of interaction between their components. This complexity comes into the sharpest focus if one tries to develop a mathematical, computer-checkable proof that a concurrent program produces the desired result. The required effort for developing such a proof today is overwhelming even for the simplest concurrent programs, because of the combinatorial explosion associated with the component interaction.

The goal of the Mathador project is to study, decompose, and simplify the structure of mathematical proofs of concurrent programs, to the point where they can be developed on a regular basis. Mastering these proofs will mean that we know how to describe the interaction between concurrent components in an intellectually manageable way. In turn, this will directly impact how we think about, write, and understand concurrent software.

The starting point in this task is the well-known idea in theoretical computer science that programs and mathematical proofs share common foundations in constructive mathematics. One can thus apply programming ideas, such as abstraction and information hiding, to control the combinatorial explosion that is inherent in proofs. The project's goal is then to develop constructive mathematical theories that will facilitate engineering of practically feasible computer-checkable proofs for concurrent programs.

The Mathador project is supported by an ERC Consolidator Grant awarded to Aleks Nanevski for 2017-2021.

concurrent software verification

structures for

Related publications

[1] Aleksandar Nanevski. *Separation Logic and Concurrency*. Lecture notes for Oregon Programming Languages Summer School (OPLSS'16), June 2016. https://software.imdea.org/~aleks/oplss16/notes.pdf

[2] Ruy Ley-Wild and Aleksandar Nanevski. *Subjective auxiliary state for coarse-grained concurrency*. Proceedings of the 40th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL'13), pages 561–574, ACM Press, 2013.

[3] Ilya Sergey, Aleksandar Nanevski and Anindya Banerjee. *Mechanized Verification of Fine-grained Concurrent Programs*. Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'15), pages 77-87, ACM Press, 2015.

homomorphic

at WORKS

Homomorphic Cryptocomputing at Works

HC@WORKS (Homomorphic Cryptocomputing at WORKS) focuses on accelerating the time to market of recently developed cryptographic techniques for protecting data privacy in real-world highly innovative software products. HC@WORKS is an innovation action funded by EIT Digital (formerly known as EIT ICT Labs) during 2015 and 2016. The HC@WORKS consortium comprises 6 European partners: three technology providers from the academic world (CEA LIST from France, CNR from Italy and the IMDEA Software Institute) and three use case providers from the Industry (Atos from Spain, Engineering from Italy, and Thales from France).

The main goal of HC@WORKS is to develop a suite of software tools that enable the execution of algorithms directly on encrypted data (namely, without the need to decrypt during the computation) by using *homomorphic encryption techniques*. Computing directly on encrypted information is indeed a key enabler for solving a number of privacy issues that arise when processing sensitive data on untrusted cloud computing platforms. The action focuses on maturing the complementary technologies developed by the academic partners (compiler and runtime environment for homomorphic encryption by CEA LIST, platform for multiparty computation by CNR, and verifiable computation techniques by

cryptocomputing

IMDEA Software Institute), and applying them to three independent applications brought by the Industrial partners. The three applications are in the field of healthcare (Atos), cybersecurity (Thales) and open data analytics (Engineering) where privacy-preserving solutions are of crucial importance, and the innovative technologies developed in HC@ WORKS will enable the creation of new privacy-enhanced versions of these products and services.

The IMDEA Software Institute joined the consortium in 2016 to provide the verifiable computation technologies [1] that, in addition to enable computing on encrypted data, bring to the applications further security by means of unforgeable integrity checks.

Related publications

[1] D. Fiore, V. Pastro, and R. Gennaro. Efficiently Verifiable Computation on Encrypted Data. In *ACM CCS 2014 – 21th ACM Conference on Computer and Communication Security*, pages 844–855, 2014.

smart mobi

Smart Mobile APP PERmission management

permission management

SMAPPER (Smart Mobile APP PERmission management) is a one year-long innovation action funded by the EIT Digital activities in 2016 in the Privacy, Security and Trust action line. The action focuses on the development of a novel technology that estimates the security and privacy risk level of Android mobile applications. This action primarily targets non-expert users, who can hardly understand and control how apps behave and access sensitive data on their devices.

The main contribution of SMAPPER is a back-end service comprising several components to statically analyze mobile applications at the bytecode level. The anomaly detection component, developed by IMDEA Software Institute, reports anomalous permission requests using a combination of natural language processing and machine learning techniques; the information flow component, developed by Saarland University, analyzes how applications use sensitive information such as the user's location or phone number, and reports information leaks; the risk estimator component, developed by Telecom Italia, reports possible man-in-the-middle exposures, unused permissions, and native code usage.

Two Android apps, which are also designed and developed within this project, leverage on the SMAPPER back-end service to warn users about possibly risky applications, and to let them block risky or undesired functionalities. The first mobile application is currently used by Telecom Italia employees, and the company is evaluating possible strategies to make it available as a service for their customers. The second application is a new release of AppGuard, an existing technology developed by the Backes SRT company, a startup based in Germany. AppGuard currently counts over 7000 active users.

The partners involved in the action are Telecom Italia (Italy), Saarland University (Germany), and Backes SRT (Germany). Alessandra Gorla and Juan Caballero from the IMDEA Software Institute are the coordinators of the action.

le app

Related publications

[1] A. Gorla, I. Tavecchia, F. Gross, and A. Zeller. Checking App Behavior Against App Descriptions. In *ACM/IEEE ICSE 2014 – 36th International Conference on Software Engineering*, pages 1025—1035, 2014.

[2] V. Avdiienko, K. Kuznetsov, A. Gorla, A. Zeller, S. Arzt, S. Rasthofer, and E. Bodden. Mining Apps for Abnormal Usage of Sensitive Data. In *ACM/IEEE ICSE 2015 – 37th International Conference on Software Engineering*, pages 426—436, 2015.

[3] V. Avdiienko, K. Kuznetsov, P. Calciati, J. C. Caiza Román, A. Gorla, and A. Zeller. CALAPPA: a Toolchain for Mining Android Applications. In *ACM WAMA 2016 – 1st International Workshop on App Market Analytics*, pages 22—25, 2016.

architecture-dri

of systems software

Architecture-Driven Verification of Systems Software

The research in architecture-driven verification of system software at the IMDEA Software Institute is performed in part within the scope of the EU project ADVENT, an FP7 FET Young Explorers project started in 2013 and coordinated by IMDEA Software in cooperation with Katholieke Universiteit Leuven (Belgium), Max Planck Institute for Software Systems (Germany) and Tel-Aviv University (Israel). The research is also supported by a Microsoft Software Engineering Innovation Foundation Award and a Microsoft European Ph.D. Scholarship.

The key element of the ADVENT approach is to base the design of advanced verification techniques on formalization of software engineering concepts already used by systems programmers to reason about their software informally. By taking advantage of programmers' knowledge and intuition, this approach improves on the common practice of building generic verification tools that fail to scale to big and complicated systems.

The architecture-driven techniques have the potential to result in verification tools that require a minimal and intuitive user input — essentially equivalent to a formal version of the high-level informal specifications programmers already have in mind when developing software. In time, this can yield a dramatic leap in the cost-benefit ratio of the verification technology, allowing it to scale to systems of real-world size and complexity that have so far been beyond the reach of quality assurance methods for guaranteeing correctness.

ven verification

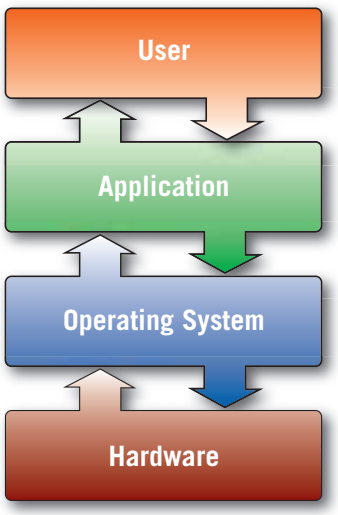




Related publications

[1] *Artem Khyzha*, *Alexey Gotsman*, and Matthew Parkinson A generic logic for proving linearizability. FM'16: International Symposium on Formal Methods, Limassol, Cyprus, LNCS 9995, pages 426-443. Springer, 2016.

[2] *Alexey Gotsman* and Hongseok Yang. Composite replicated data types. ESOP'15: European Symposium on Programming, London, UK, LNCS 9032, pages 585-609. Springer, 2015.



editor
imdea software institute

graphic design
base 12 diseño y comunicación

photos on pages 13 and 14
Daniel Schäfer

legal deposit number
M-2812-2017

Comunidad de Madrid

EUROPEAN UNION
STRUCTURAL FUNDS

imdea **software** institute

annual report

2016

www.software.imdea.org

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